

**This Page Is Inserted by IFW Operations
and is not a part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.

Parallel pseudo-random generator for emulating a serial pseudo-random generator and method for carrying out same.

Patent Number: EP0397079, A3

Publication date: 1990-11-14

Inventor(s): ROGER GEORGE ANDRE CHARLES (FR); POWELL WILLIAM EDWARD (US); WEEBER WILLIAM BERNARD (US)

Applicant(s): ALCATEL NV (NL)

Requested Patent: JP3068022

Application Number: EP19900108555 19900507

Priority Number (s): US19890351175 19890512

IPC Classification: H04L25/49

EC Classification: H04L25/03E3

Equivalents: AU5495690, AU629933, CA2016635, US5031129

Cited patent(s): US4965881

Abstract

A parallel pseudo-random generator for emulating a serial pseudo-random generator that generates serial outputs such that the next serial output value is based upon an Exclusive OR combination of at least two preceding serial output values the maximum preceding serial output value defined as the Pth preceding serial output value, where P is an integer greater than one; comprising: A) at least P latches, each latch having an output having a logic value 1 or 0 and an input operable upon receipt of a clock signal, for receipt of data for controlling the next logic value on the latch output; B) at least P Exclusive OR gates, each having at least two inputs and one output, each Exclusive OR gate output connected to a corresponding input of one latch so as to define the next value of the latch output upon receipt of the next clock signal; and C) means for connecting each input of each Exclusive OR gate to one latch output so that the output of each Exclusive OR gate represents the corresponding next value of the latch to which this Exclusive Or gate output is connected.

Data supplied from the esp@cenet database - I2

⑯ 公開特許公報 (A)

平3-68022

⑮ Int. Cl. 5

G 06 F 7/58
H 03 K 3/84

識別記号

庁内整理番号

B 7056-5B
A 8626-5J

⑯ 公開 平成3年(1991)3月25日

審査請求 未請求 請求項の数 4 (全31頁)

⑭ 発明の名称 直列疑似乱数列生成機をエミュレートするための並列疑似乱数列生成機及びその実行方法

⑯ 特願 平2-122861

⑯ 出願 平2(1990)5月11日

優先権主張 ⑯ 1989年5月12日 ⑯ 米国(US)⑯ 351,175

⑯ 発明者 ウィリアム・エドワード・ポーウエル アメリカ合衆国、ノース・カロライナ・27614、ローリー、

⑯ 発明者 ウィリアム・バーナード・ウエバー アメリカ合衆国、ノース・カロライナ・27502、アベック

⑯ 出願人 アルカテル・エヌ・ベー オランダ国、1077・イツクス・イツクス・アムステルダム、ストラビンスキーラーン・341

⑯ 代理人 弁理士 川口義雄 外2名
最終頁に続く

明細書

1. 発明の名称

直列疑似乱数列生成機をエミュレートするための並列疑似乱数列生成機及びその実行方法

2. 特許請求の範囲

(1) 次の直列出力値が少なくとも2つの先行の直列出力値の排他的ORの組合せに基づくような直列出力を生成する直列疑似乱数列生成機をエミュレートするための並列疑似乱数列生成機であって、最大の先行直列出力値がP番目(但しPは1よりも大きい整数である)の先行の直列出力値として定義されており。

A) 各々が、論理値1または0を有する出力と、前記出力において次の論理値を抑制するためにデータを受信するようにクロック信号受信時に動作可能な入力とを有する少なくともP個のラッチと、

B) 各々が少なくとも2つの入力と1つの出力を有する少なくともP個の排他的ORゲートであって、該排他的ORゲートの各々の出力が、次のクロック信号受信時に前記ラッチの出力の次の値を定義するように、1つのラッチの対応する入力に接続されている排他的ORゲートと、

C) 前記排他的ORゲートの各々の出力が、この排他的ORゲートの出力が接続されているラッチの対応する次の値を与えるように、前記排他的ORゲートの各々の入力を1つのラッチの出力に接続する手段

とを包含する並列疑似乱数列生成機。

(2) 前記直列疑似乱数列生成機を定義する直列排他的OR組合せが、(Pを7とすると)6番目及び7番目の先行の直列出力値に基づいてその次の出力値を決定する請求項1に記載の並列疑似乱数列生成機。

(3) 前記ラッチの数が8であり、該ラッチが対応する出力Q0からQ7を有しており、各々が対応するラッチの入力に接続されている出力を有する対応する排他的ORゲートEx0からEx7の入力が、

Ex0の入力がQ4及びQ6に接続され、

Ex1の入力がQ5及びQ7に接続され、

Ex2の入力がQ0及びQ1に接続され、

Ex3の入力がQ1及びQ2に接続され、

Ex4の入力がQ2及びQ3に接続され、

Ex5の入力がQ3及びQ4に接続され、

Ex6の入力がQ4及びQ5に接続され、

Ex7の入力がQ5及びQ6に接続される

ようにラッチの出力に接続されている請求項2に記載の並列疑似乱数列生成器。

(4) 前記直列疑似乱数列生成器を定義する直列排他的OR組合せが、6番目及び7番目の先行の直列出力を組合せるものであり、前記ラッチの数が16であり、前記ラッチは対応する出力Q0～Q15を

Ex14の入力がQ4及びQ5に接続され、

Ex15の入力がQ5及びQ6に接続される

ようにラッチの出力に接続されている請求項1に記載の並列疑似乱数列生成器。

3. 発明の詳細な説明

技術分野

本発明は、直列疑似乱数列生成器(PRG)またはスクランbler(scrambler)の出力を、直列PRGの巡続する直列出力を与える複数の出力を備えた並列実現態様によりエミュレートするための回路及びその方法に関する。本発明は特に、適正な刻時(clocking)を保証するため及びデータストリームの潜在的な機密保護のために、高速データストリームを直列PRGと組み合わせる通信において使用される。このような通信データは高速であるが故に、直列PRGを相補形金属酸化物シリコン(CMOS)回路を使用して実現することはできない。従って、回路のクロック速度がCMOS回路の動作周波数内で

有しており、該並列疑似乱数列生成器の幅が16に等しく、更に、各々が対応するラッチの入力に接続されている出力を有する対応する16個の排他的ORゲートEx0～Ex15の入力が、

Ex0の入力がQ8及びQ12に接続され、

Ex1の入力がQ9及びQ13に接続され、

Ex2の入力がQ10及びQ14に接続され、

Ex3の入力がQ11及びQ15に接続され、

Ex4の入力がQ0及びQ2に接続され、

Ex5の入力がQ1及びQ3に接続され、

Ex6の入力がQ2及びQ4に接続され、

Ex7の入力がQ3及びQ5に接続され、

Ex8の入力がQ4及びQ6に接続され、

Ex9の入力がQ5及びQ7に接続され、

Ex10の入力がQ0及びQ1に接続され、

Ex11の入力がQ1及びQ2に接続され、

Ex12の入力がQ2及びQ3に接続され、

Ex13の入力がQ3及びQ4に接続され、

あるように、直列PRGをエミュレートする必要がある。

発明の背景

同期光網仕様(SONET)が採用されてから高速ディジタル通信に対する規格が設けられた(参照: American National Standards Institute, Inc.

"Digital Hierarchy Optical Interface Rates and Formats Specification" 規格 TI.105-1988)。

典型的にはこのようなディジタル通信は、データストリームが多数の隣合った0と1とで構成されている場合に、そうしなければ生じ得るであろうクロック信号の損失の可能性を最小化するために、疑似乱数列の直列スクランブル信号をデータストリームと組み合わせる。しかしながら直列データストリームは1秒当たり155メガビットまたはそれ以上で動作し得るので、直列PRGは、製造がより安価であり且つ対応するエミッタ結合論理(ECL)またはヒ化ガリウム(GaAs)回路より低い電力で動作

する好ましいCMOS回路ではなくて、個別のECL回路、ECL適用業務特定集積回路(ECL ASIC)またはヒ化ガリウム回路のような高速製造技術を使用して実現される必要がある。ECL及びGaAs回路の付加製造コスト及び電力要求は、付加的な熱を散逸するためにプリント回路基板面積をより大きくする必要があり、またもやCMOS回路、特にCMOS適用業務特定集積回路(CMOS ASIC)が好ましくなる。

CMOS回路は典型的には50メガビットより速いクロック速度で動作できないので、直列疑似乱数列生成器のクロック周波数を効果的に小さくするためにある技術を使用することが必要である。本発明は、かかる技術と、任意の直列PRGの生成多項式に対して、及び等価の直列シフトレジスタの長さよりも大きい任意のサイズの、直列PRGからの連続出力を与える並列出力ワードに対して動作可能の回路を提供する。

こうして、比較的コストが低く電力消費量がよ

並列PRGは、直列PRGを効果的にエミュレートする帰還経路を選択することにより任意の数の出力(任意の大きさのM)に拡張することができる。帰還経路は直列生成多項式と並列PRG実現態様の出力の大きさとに基づいている。それぞれMが8及び16の本発明の2つの好ましい実施例においては、対応する数のD型フリップフロップ(FF)を、シミュレートされる直列PRGの次のM個の逆続する値に対応する次のM個の出力の値を決定するのに必要な帰還を提供する排他的OR(XOR)ゲートと一緒に使用する。これら2つの実現態様は、直列疑似乱数列生成器をシミュレートするため最小数の排他的ORゲートに対して設定された最適化基準を使用することにより最適化される。

発明の目的

本発明の目的は、M個の並列出力が直列疑似乱数列生成器のM個の逆続出力値をエミュレートするための、直列疑似乱数列生成器の出力をシミュ

リ小さなCMOS回路を、直列PRGの出力をエミュレートする並列PRGを製造するために使用することができる。

発明の概要

並列疑似乱数列生成器は、直列PRGの次の入力値が直列PRGの複数の先行の出力の排他的OR(XOR)の組合せに等しい帰還構成において次々と動作する直列疑似乱数列生成器をエミュレートするものと説明される。例えば通信において典型的なスクランブル多項式は $1 + X^4 + X^7$ である。この多項式は、直列PRGの次の入力値が、該生成器の5番目の先行の値と該生成器の7番目の先行の値とを排他的OR演算した出力に等しいことを意味する。生成器の7番目の値の出力も典型的には、スクランブルされるべきデータと排他的OR演算されている。

もし直列PRGがクロック速度 f_s を有するならば、並列PRGはクロック速度 $f_p = f_s/M$ は並列PRGの出力の数である]を有する。

レートする並列疑似乱数スクランブル回路とその方法とを提供する。

本発明の別の目的は、得られる並列クロック周波数が任意に低く設定され得、従ってCMOS製造技術を使用して並列PRGの実現態様を提供し得るようMの値を任意の大きさにすることができる前記並列PRGを提供することである。

本発明の更に別の目的は、次のM個の出力を決定するためにM個の出力から必要な帰還を提供するための排他的ORゲートと一緒にD型フリップフロップを組み込んだ前記並列PRGを提供することである。

本発明の更に別の目的は、任意の直列PRG生成多項式に対して実行可能な前記並列PRGを提供することである。

本発明の他の目的は以下に明らかとなるであろう。

本発明の特徴及び目的がより充分に理解される

表1

2つの入力に対する排他的ORゲートの真理表

X ₁	X ₂	f
0	0	0
0	1	1
1	0	1
1	1	0

 X_1 及び X_2 は入力であり、fは出力である。

(これは、繰上げのない2を法(モジュロ)とする和算に等価である。)

ほとんどの通信適用業務における疑似乱数列生成機の目的は、通信ビットストリームパターンとは無関係に、伝送される実際の情報がおおよそ同じ数の1と0とを含むことを保証することである。こうすると、例えばもし通信ビットストリームが長く連続する1または0のパターンを含むならばより困難になるであろう通信ビットストリームにおけるクロック情報の保守管理が容易となる。このようなスクランブルはデータ暗号化にも有効である。

る。

再度第1図を参照すると、直列疑似乱数列生成機の動作は典型的には多項式：

$$1 + X^a + \cdots + X^b$$

で定義され得ることが判る。これは、「+」が排他的OR演算を意味する特性多項式として公知である(本明細書中では全てこのように使用するものとする)。

この特性多項式に関係する帰還方程式は、

$$X^a + X^b + \cdots + X^0 = 0$$

として説明される。上記式から、

$$X^a + X^b + X^c + \cdots + X^0 = 0 + X^0$$

となるが、一般に「+」が排他的OR演算子であると $X + X = 0$ 及び $0 + X = X$ であるので、

$$X^a + \cdots + X^0 = X^0$$

となる。この方程式は、シフトレジスタの次の入力値が $X^a + \cdots + X^0$ であることを意味する。

例えば同期光網(SONET)規格(American National

Standards Institute(ANSI)規格 TI.105-1988

としても公知である)においてはこの多項式は $1 + X^a + X^b$ である。第1図から判るように、この多項式は、シフトレジスタ6における値がレジスタ7における値と排他的OR演算され、その結果がP段シフトレジスタの段1における次の値となることを意味する。表4は、7段シフトレジスタの各段に対する出発値が論理値1である場合の7つの段における値を示す。この出発値は典型的には「シード(seed)」と称される。SONET規格においては、シードは典型的には直列PRGに対して全て1である。これから判るように、段1に対して生成される値はシフトレジスタの段を連続的に移動する。前記したように、段7からの出力は直列通信ビットストリームと排他的OR演算するためにも使用される。

このような生成機が疑似乱数列生成機と称される理由は、生成されるビットストリームが同じ出

発シード及び同じ多項式に対して常に同じであるからである。

SONET多項式は段6及び7の排他的OR演算を使用したが、勿論、直列シフトレジスタの異なる段を合わせて排他的OR演算する他の多項式を使用することもできる。実際、所望であれば2つ以上の段を排他的OR演算してもよい。

一般には最大長の多項式、即ち最大カウント(クロックサイクル)後にそれ自体を繰り返す多項式が使用される。最大長の多項式に対するカウントの最大数は、n次多項式において $2^n - 1$ である。例えば、3次の多項式では最大多項式は $1 + X^2 + X^3$ であり、非最大多項式は $1 + X^1 + X^2 + X^3$ である。表2及び3から判るように、最大長多項式は7つの出力の後に繰り返し、一方、非最大長多項式は4つの出力の後に繰り返す。

本発明は、最大であろうとなからうと任意の直列多項式を用いて適用可能である。

メガビット/秒を越える速度では、相補形金属酸化物シリコン(CMOS)集積回路の製造は非実用的になる。実際に、使用可能速度が約75メガヘルツを越えるCMOSの製造は実質的に不可能である。結果としてSONET標準に使用されるもののような高い伝送速度(例えば155メガビット/秒)に対しては、このような直列疑似乱数列生成機を使用するのであれば、エミッタ結合論理(ECL)またはヒ化ガリウム(GaAs)技術を使用して製造することが必要となる。上記両技術はCMOS技術と比較して、典型的には製造がより難しく、より多くの熱を生成するので発生した熱を散逸するための集積回路素子を設置するためにより大きな面積のプリント回路基板を必要とし、1論理ゲート当たりのコストがより高くなるという深刻な欠点を有する。

本発明は、その確が直列疑似乱数列生成機の連続出力を与える複数の並列出力を有する並列疑似乱数列生成機を提供することにより、高速度疑似

表2

次数3の多項式

 $X^2 + X^3$ (最大長= $2^3 - 1 = 2^3 - 1 = 8 - 1 = 7$)

表3

次数3の多項式

 $X^1 + X^2 + X^3$

直列段番号				直列段番号							
(クロックサイクル)				1	2	3	(クロックサイクル)	1	2	3	
1	0	1	1		1	0	1	1	0	0	1
2	0	0	1		2	0	0	1	0	1	0
3	1	0	0		3	1	0	0	1	0	0
4	0	1	0		4	1	1	0	1	1	0
5	1	0	1		5	0	1	1	0	1	1
6	1	1	0		6	等					
7	1	1	1								
8	0	1	1								
9											

このような直列疑似乱数列生成機は、通信ビットストリームの伝送速度が約50メガビット/秒を越えると集積回路の実現態様に問題が生じる。50

ランダムビットパターンの生成に対する一般的な解決策を提供する。かかる並列疑似乱数列生成機24は任意の所望の数の並列出力を有することができ、第2図に示した実施例では8個の出力を有しております、第4図に示した実施例では16個の出力を有している。並列疑似乱数列生成機のサイズは、並列ワードのサイズがスクランブル多項式の次数に等しいかまたはそれより大きい限りは、特定の適用業務に最も適した任意の値に設定することができる。デジタル集積回路を使用する場合には、出力の数は一般に2の倍数に等しい値を有し、例えば8個、16個等の出力を有する。

第2図に示した実施例においては、疑似乱数列生成機は、その出力(Q0~Q7)が、エミュレートされる直列疑似乱数列生成機の8個の連続出力値を与える8個のラッチ26を有する。ラッチ26はD型のフリップフロップとすることができる。直列疑似乱数列生成機の出力が直列段7である表4を参考

照すると、この7番目の段は最初の7つの直列クロックサイクル(直列クロックサイクル0～6)に対しては論理値1を有し、次のクロックサイクル(直列クロックサイクル7)に対しては論理値0を有することが判る。従って8ビット並列PRGの出力Q7～Q0は、表5に示したように直列PRGにおける段7の8個の連続出力値を与えることができる。即ち表5から、Q0出力はこの直列PRG出力段7の8番目の直列出力を与え、Q1は段7の7番目の直列出力を与える等、同様にQ7までこの直列PRGの段7の最初の直列出力を与える。このパターンが新たな並列出力の各々に対して繰り返される。

以下に記載するように、並列PRGの次の8つの出力Q7～Q0は値00000100を有する。これらQ7～Q0に対する値は、表4に表された段7の時間出力8～15を、並列クロックサイクル1に対する並列出力(表5参照)と比較することから判るように、直列段7の次の8個の直列出力を与える。従って並

列PRGの最初(0番目)のフレームは直列PRGの段7の最初の8つの直列出力(直列クロックサイクル)に対応しており、並列PRGのフレーム1は段7の次の8つの直列出力(直列クロックサイクル8～15)に対応する等となる。最初の並列フレームは、それ自体が特定の出発シーケンスまたはシードを有する直列PRGをエミュレートする上でその動作を開始するための、生成機への並列シード入力である。

表4

1+X⁶+X⁷生成多項式に対応する直列疑似乱数列発生機

時間 (各箇の直列クロックサイクル)	直列段番号 1 2 3 4 5 6 7
0	1 1 1 1 1 1 1
1	0 1 1 1 1 1 1
2	0 0 1 1 1 1 1
3	0 0 0 1 1 1 1
4	0 0 0 0 1 1 1 (並列フレーム0 (8ビットの場合))
5	0 0 0 0 0 1 1
6	0 0 0 0 0 0 1
7	1 0 0 0 0 0 0
8	0 1 0 0 0 0 0
9	0 0 1 0 0 0 0
10	0 0 0 1 0 0 0
11	0 0 0 0 1 0 0
12	0 0 0 0 0 1 0
13	1 0 0 0 0 0 1
14	1 1 0 0 0 0 0
15	0 1 1 0 0 0 0
16	0 0 1 1 0 0 0
17	0 0 0 1 1 0 0
18	0 0 0 0 1 1 0
19	1 0 0 0 0 1 1 (並列フレーム2)
20	0 1 0 0 0 0 1
21	1 0 1 0 0 0 0
22	0 1 0 1 0 0 0
23	0 0 1 0 1 0 0
24	0 0 0 1 0 1 0
25	1 0 0 0 1 0 1
26	1 1 0 0 0 1 0
27	1 1 1 0 0 0 1 (並列フレーム3)
28	1 1 1 1 0 0 0
29	0 1 1 1 1 0 0
30	0 0 1 1 1 1 0
31	1 0 0 1 1 1 1

表4(続き)

1+X⁶+X⁷生成多項式に対応する直列疑似乱数列発生機

時間 (各箇の直列クロックサイクル)	直列段番号 1 2 3 4 5 6 7
32	0 1 0 0 1 1 1
33	0 0 1 0 0 1 1
34	0 0 0 1 0 0 1
35	1 0 0 0 1 0 0
36	0 1 0 0 0 1 0
37	1 0 1 0 0 0 1
38	1 1 0 1 0 0 0
39	0 1 1 0 1 0 0
40	0 0 1 1 0 1 0
41	1 0 0 1 1 0 1
42	1 1 0 0 1 1 0
43	1 1 1 0 0 1 1 (並列フレーム4 (16ビットの場合))
44	0 1 1 1 0 0 1
45	1 0 1 1 1 0 0
46	0 1 0 1 1 1 0
47	1 0 1 0 1 1 1
48	0 1 0 1 0 1 1
49	0 0 1 0 1 0 1
50	1 0 0 1 0 1 0
51	1 1 0 0 1 0 1 (並列フレーム5)
52	1 1 1 0 0 1 0
53	1 1 1 1 0 0 1
54	1 1 1 1 1 0 0
55	0 1 1 1 1 1 0

表5

$! \cdot X^* \cdot X^*$ 生成多項式に対応する直列PRGをエミュレートする並列疑似乱数列生成機(幅=8ビット)

組	直列	並列出力						
		Q0	Q1	Q2	Q3	Q4	Q5	Q7
0	0 - 7	0	1	1	1	1	1	1
1	8 - 15	0	0	1	0	0	0	0
2	16 - 23	0	0	0	1	1	0	0
3	24 - 31	1	0	0	0	1	0	1
4	32 - 39	0	0	1	0	0	1	1
5	40 - 47	1	0	0	1	1	0	1
6	48 - 55	0	0	1	0	1	0	1

$$F2 = Q0 + Q1$$

$$F3 = Q1 + Q2$$

$$F4 = Q2 + Q3$$

$$F5 = Q3 + Q4$$

$$F6 = Q4 + Q5$$

$$F7 = Q5 + Q6$$

第2図においては更に並列疑似乱数列生成機の出力Q0～Q7は、対応する数のデータストリーム出力排他的ORゲート30に次々と与えられることが判る。排他的ORゲート30においては、各排他的ORゲートへの第2の入力には、Q7の排他的OR出力ゲート30'への入力は直列データの最初のビットと排他的OR演算され、出力Q6は直列データの次のビットと排他的OR演算される等、Q0が直列データの8番目のビットと排他的OR演算されるように、直列データストリームの1つのビットが与えられる。従って出力線32における出力信号は、8ビットマルチプレクサ(図示なし)を使用することにより直

直列PRGをシミュレートするための並列実現態様

解説

第2図から判るように、ラッチ28に加えて並列PRGには更に複数の排他的ORゲート28が組み込まれており、排他的ORゲート28は、ラッチが次の出力を生成するようにラッチへ入力として与えるためにラッチの種々の出力を組合わせる。第3図は生成機を起動し(ANDゲート34)、並列シードをコードし(ORゲート36)、且つ並列クロック信号38を与えるための追加論理回路を示す第2図に対応する概略図である。

第2図から判るように、8つのフリップフロップの入力D0～D7には関数F0～F7に関係する値が与えられる。これらの関数は表5Aに示した方程式で定義される。

表5A

$$F0 = Q4 + Q6$$

$$F1 = Q5 + Q7$$

列ビットストリームに交換し直され得るスクランブルされた出力データを与える。

第2図から、もし並列疑似乱数列生成機が幅8(W=8)を有するならば、シミュレートされた直列疑似乱数列生成機の次の8つの出力をそれぞれQ7～Q0で与えられるように各々の並列計算がなされるので、並列動作の周波数は到来する直列ビットストリームのものの8分の1となることは容易に判る。

並列出力排他的OR組合せの決定

以下により充分に説明するように、並列疑似乱数列生成機の各ラッチへの入力を与えるための排他的ORゲート構成は、直列疑似乱数列生成機の出力ビットストリームをエミュレートするように決定される。第2図には特定の排他的ORゲート構成を示してあるが、実際には多くの実現態様が可能である。本発明は、各入力に対して最小数の排他的ORゲートを使用する場合に特に有利である。こ

の構成は、直列ゲートに対する必要条件を最小化し、結果として各直列ゲートに付随するゲート遅延を最小化する。

任意の疑似乱数列生成機の多項式に対して、並列PRFの値が、直列PRGの多項式を定義するのに使用される最大シフトレジスタ段に少なくとも等しいという条件で、排他的ORゲートを並列疑似乱数列生成機を実行するために使用することができる解決策が存在することは、経験的に見出されており、本明細においても発明者C.Rogerによる標題「並列疑似乱数列発生機、数学的解析(Parallel Pseudo-Random Generator, Mathematical Analysis)」の数学的解析のなかに記載されているように数学的検証もされている。

第1図に関して与えられた上記多項式、即ち段1への次の入力が段6及び7の排他的OR出力に等しい多項式においては、この関係は一般に、

$$Q(n) \equiv Q(n+6) + Q(n+7) \quad (1)$$

6参照)。即ち8ビット並列PRGの実現態様においては、Q7に対する次の値はQ-1に等しく、従ってQ5及びQ8の排他的ORに等しいことになる。即ち、次のQ7 = F7 = Q5 + Q6である。

この同じ関係を用いてQ6～Q2の次の値は以下のように定義され得る。即ち、

$$\text{次の } Q6 = F6 = Q4 + Q5,$$

$$\text{次の } Q5 = F5 = Q3 + Q4,$$

$$\text{次の } Q4 = F4 = Q2 + Q3,$$

$$\text{次の } Q3 = F3 = Q1 + Q2,$$

$$\text{次の } Q2 = F2 = Q0 + Q1$$

となる。

Q1の数値の求め方は表6及び第7図を参照することにより最も良く理解され得る。

〔式中のnは直列PRGの任意の段である〕

と定義され得ることが判る。第7図はこの関係を図で表したものである。

再度表4を参照すると、クロックサイクル0に対する段6及び7がともに論理値1を有することが判る。その結果、段1に対する次の値は0となる($1 + 1 = 0$ (表1参照))。この結果は、nが0である場合の上記式と同等となる(次の直列クロックサイクル後にはQ(0)はQ(1)となり、一般に次の直列クロックサイクル後にはQ(n-1)はQ(n)となる)。

エミュレーション用8出力並列疑似乱数列生成機の次の8ビットを決定するためには、直列PRGの次に生成されるビットが、8直列クロックサイクロ後に並列PRGの出力Q7に対する次の値となることが判る(Q-1は、1直列クロックサイクル後にQ0となり、更に7直列クロックサイクル後にQ7となり、これら8つの直列クロックサイクルは1つの並列ワードクロックサイクルと等価である(表

表6

2つの8ビットワードに対する並列出力値
(n = -8～n = 7)

Q-8 Q-7 Q-6 Q-5 Q-4 Q-3 Q-2 Q-1 | Q0 Q1 Q2 Q3 Q4 Q5 Q6 Q7
次の8ビットワード 現在の8ビットワード

従って、(F1と等値の)Q1に対する次の値はQ-7の値に等しい。即ち、

$$\text{次の } Q1 = F1 = Q-7$$

である。式(1)から、

$$F1 = Q(-7 + 6) + Q(-7 + 7) = Q-1 + Q0 \quad (n = -7)$$

となるが、(式(1)を再度使用すると)、

$$Q-1 = Q5 + Q6 \quad (n = -1)$$

であるので、

$$\text{次の } Q1 = F1 = Q-1 + Q0 = Q5 + Q6 + Q0$$

と書ける。しかしながら更に式(1)から、Q0の現在の値はQ6 + Q7の現在の値に等しい($Q0 = Q6 + Q7$)ので、

$$\text{次の } Q1 = F1 = Q5 + Q6 + Q6 + Q7 \quad (2)$$

となる。全ての論理値のそれ自体の排他的ORは0となるので(表1参照)、式(2)は、

$$\text{次の } Q1 = F1 = Q5 + Q7$$

と書き換えることができる。

同じ原理を使用し、Q0の次の値は、

$$\text{次の } Q0 = F0 = Q4 + Q6$$

と定義されることは容易に明らかである。

従って、排他的ORゲート構成を決定するための方法に不可欠なことは、直列生成多項式によって直列段間の相関関係を決定することである。並列関係は単に複数の直列段を同時に与えるものであるので、Kを並列出力の幅(即ち数)とするとK個の直列クロックサイクル後の並列出力の各々に対して次の並列出力を計算するために、直列多項式を使用する。並列出力段の現在の値のみが、かかる同じ段の次の値を計算するために使用可能であるので、出力値が並列PRGの1つ以上の次の出力(表6に示した次のワード)から要求されるのであれ

16ビット並列PRG		現在の16ビットワード
16-15-14-13-12-11-10-9-8-7-6-5-4-3-2-1	0-1-2-3-4-5-6-7-8-9-10-11-12-13-14-15	
Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q	Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q	次の16ビットワード

ば、次の出力値を与える現在の出力を決定する特定の出力に対して直列多項式を再度使用する。この方法はいかなるサイズの並列ワードに対してもまたいかなる直列生成多項式に対しても使用することができる。

表7を参照すると、16ビット並列PRGの実現態様において、Q15の次の値は単にQ-1(即ち16直列クロックパルス後の直列出力)に等しい。即ち、

$$\text{次の } Q15 = F15 = Q-1 = Q5 + Q6 \quad (n = -1 \text{に対する式(1)参照})$$

である。

この解析はQ14～Q10の次の値に対しても成立する。即ち、

$$\text{次の } Q14 = F14 = Q4 + Q5$$

$$\text{次の } Q13 = F13 = Q3 + Q4$$

$$\text{次の } Q12 = F12 = Q2 + Q3$$

$$\text{次の } Q11 = F11 = Q1 + Q2$$

$$\text{次の } Q10 = F10 = Q0 + Q1$$

である。Q9の次の値はF9、つまりQ-1+Q0に等しいことが判るが、Q-1は単にQ5+Q6に等しいので、

$$\text{次の } Q9 = F9 = Q5 + Q6 + Q0$$

となる。Q0の現在の値は式(1)によってQ6+Q7に等しく、従って、

$$\text{次の } Q9 = F9 = Q5 + Q6 + Q6 + Q7$$

$$\text{次の } Q9 = F9 = Q5 + Q7$$

となる。同様にQ8～Q4の次の値に対しては、

$$\text{次の } Q8 = F8 = Q4 + Q8$$

$$\text{次の } Q7 = F7 = Q3 + Q5$$

$$\text{次の } Q6 = F6 = Q2 + Q4$$

次の $Q_5 = F_5 = Q_1 + Q_3$ 次の $Q_4 = F_4 = Q_0 + Q_2$

である。

Q_3 の次の値は $Q-13$ に等しい。上記式(1)を使用すると、

次の $Q_3 = F_3 = Q-13$

$$Q-13 = Q-7 + Q-6 \quad (n = -13)$$

$$Q-13 = (Q-1 + Q_0) + (Q_0 + Q_1)$$

$$Q-13 = Q-1 + Q_1$$

$$Q-13 = (Q_5 + Q_6) + Q_1$$

$$Q-13 = (Q_5 + Q_6) + (Q_7 + Q_8) \quad (2a)$$

であり、更に式(1)から、

$$Q_5 = Q_{11} + Q_{12}$$

$$Q_6 = Q_{12} + Q_{13}$$

$$Q_7 = Q_{13} + Q_{14}$$

$$Q_8 = Q_{14} + Q_{15}$$

であり、従って、

$$Q-13 = (Q_{11} + Q_{12}) + (Q_{12} + Q_{13}) + (Q_{13} + Q_{14}) + (Q_{14} + Q_{15})$$

任意の幅の並列PRGに対して使用することができ。直列多項式が、次の入力段を計算するために段6及び7を使用する上記実施例においては、Pの値は7であり、即ち並列PRGの幅は少なくとも7に等しい必要があるが、これより大きくともよい。

更に、直列多項式は2つの直列段の排他的ORに等しいとしたが、本発明は、次の入力を計算するために排他的OR演算される直列段の数とは無関係に、任意の直列多項式に適用可能である。

より一般的な直列疑似乱数列生成機の例では多項式：

$$\text{次の直列入力} = X^2 + X^3 + X^4$$

を使用する。即ち特性多項式は $1 + X^2 + X^3 + X^4$ である。

この多項式は非最大(前記表2及び3参照)であるが、並列PRG実行方法が適用業務において一般的であることを示すために与えられている。

となる。即ち、

$$Q_3 = Q_{11} + Q_{15} \quad (2b)$$

である。同様に、

$$\text{次の} Q_2 = F_2 = Q_{10} + Q_{14}$$

$$\text{次の} Q_1 = F_1 = Q_9 + Q_{13}$$

$$\text{次の} Q_0 = F_0 = Q_8 + Q_{12}$$

である。

上記解析に対応する16ビット並列PRGに対する排他的OR演算実現態様は第4図に示してある。

次の Q_{13} は式(2a)及び(2b)によって示されるような複数の排他的OR演算によって定義され得ることが判る。一般に出力に対してはこのような多重表示が与えられ得る。1つの最適化基準は、出力 Q_3 に対して式(2b)で示されるような最小数のゲート入力を使用することであろう。

上記解析は、並列PRGの幅がエミュレートされる直列PRGに対する帰還構成において使用される最大数の直列段に少なくとも等しいという条件で

第8図は、段nに関して、

$$Q(n) \equiv Q(n+2) + Q(n+5) + Q(n+9) \quad (3)$$

であるこの並列疑似乱数列生成機を示す。

表8は、この多項式の36のクロックサイクル(クロックサイクル0~35)に対応する直列疑似乱数列生成機を構成する9つの段に対する直列段の値を示す。

(28,29,28)	表8 直列多項式 = 1 + X ² + X ⁵ + X ⁸ 直列段番号								
	1	2	3	4	5	6	7	8	9
0	0	1	1	1	1	1	1	1	1
1	1	0	1	1	1	1	1	1	1
2	0	1	0	1	1	1	1	1	1
3	1	0	1	0	1	1	1	1	1
4	0	1	0	1	0	1	1	1	1
5	0	0	1	0	1	0	1	1	1
6	0	0	0	1	0	1	0	1	1
7	1	0	0	0	1	0	1	0	1
8	0	1	0	0	0	1	0	1	0
9	1	0	1	0	0	1	0	1	0
10	1	1	0	1	0	0	0	1	0
11	1	1	1	0	1	0	0	0	1
12	1	1	1	1	0	1	0	0	0
13	1	1	1	1	1	0	1	0	0
14	0	1	1	1	1	1	0	1	0
15	0	0	1	1	1	1	1	0	1
16	0	0	0	1	1	1	1	1	0
17	1	0	0	0	1	1	1	1	1
18	0	1	0	0	0	1	1	1	1
19	0	0	1	0	0	0	1	1	1
20	1	0	0	1	0	0	1	1	1
21	1	1	0	0	1	0	0	0	1
22	1	1	1	0	0	1	0	0	0
23	1	1	1	1	0	0	1	0	0
24	1	1	1	1	1	0	0	1	0
25	0	1	1	1	1	1	0	0	1
26	1	0	1	1	1	1	1	0	0
27	1	1	0	1	1	1	1	1	0
28	0	1	1	0	1	1	1	1	1
29	1	0	1	1	0	1	1	1	1
30	1	1	0	1	1	0	1	1	1
31	1	1	1	0	1	1	0	1	1
32	1	1	1	1	0	1	1	0	1
33	0	1	1	1	1	0	1	1	0
34	0	0	1	1	1	1	0	1	1
35	0	0	0	1	1	1	1	0	1

$$\begin{aligned}
 &= (Q-2 + Q1 + Q5) + (Q1 + Q4 + Q8) + Q3 \\
 &= (Q0 + Q3 + Q7) + Q1 + Q5 + Q1 + Q4 + Q8 + Q3 \\
 &= Q0 + Q7 + Q5 + Q4 + Q8 \\
 &= Q0 + Q4 + Q5 + Q7 + Q8
 \end{aligned}$$

次のQ2 = F2 = Q-7 = Q-5 + Q-2 + Q2

$$\begin{aligned}
 &= (Q-3 + Q0 + Q4) + (Q0 + Q3 + Q7) + Q2 \\
 &= ((Q-1 + Q2 + Q6) + Q0 + Q4) + (Q0 + Q3 + Q7) + Q2 \\
 &= ((Q1 + Q4 + Q8) + Q2 + Q6) + Q0 + Q4 \\
 &\quad + (Q0 + Q3 + Q7) + Q2
 \end{aligned}$$

$$\begin{aligned}
 &= Q1 + Q8 + Q6 + Q3 + Q7 \\
 &= Q1 + Q3 + Q6 + Q7 + Q8
 \end{aligned}$$

次のQ1 = F1 = Q-8 = Q-6 + Q-3 + Q1

$$\begin{aligned}
 &= (Q0 + Q7 + Q5 + Q4 + Q8) \\
 &\quad + (Q1 + Q4 + Q8 + Q2 + Q6) + Q1 \\
 &= Q0 + Q7 + Q5 + Q2 + Q6 \\
 &= Q0 + Q2 + Q5 + Q6 + Q7
 \end{aligned}$$

次のQ0 = F0 = Q-9 = Q-7 + Q-4 + Q0

$$= (Q1 + Q8 + Q6 + Q3 + Q7)$$

式(3)の関係を使用することにより、第8図に示した直列疑似乱数列生成機をエミュレートする幅W=9を有する並列疑似乱数列生成機の次の出力Q0～Q8に対する値は以下のようにになる。即ち、次のQ8 = F8 = Q-1 = Q1 + Q4 + Q8
次のQ7 = F7 = Q-2 = Q0 + Q3 + Q7
次のQ8 = F8 = Q-3 = Q-1 + Q2 + Q6
= Q1 + Q4 + Q8 + Q2 + Q6
= Q1 + Q2 + Q4 + Q6 + Q8
次のQ5 = F5 = Q-4 = Q-2 + Q1 + Q5
= Q0 + Q3 + Q7 + Q1 + Q5
= Q0 + Q1 + Q3 + Q5 + Q7
次のQ4 = F4 = Q-5 = Q-3 + Q0 + Q4
= Q-1 + Q2 + Q6 + Q0 + Q4
= Q1 + Q4 + Q8 + Q2 + Q6 + Q0 + Q4
= Q1 + Q8 + Q2 + Q6 + Q0
= Q0 + Q1 + Q2 + Q6 + Q8
次のQ3 = F3 = Q-6 = Q-4 + Q-1 + Q3
+ (Q0 + Q3 + Q7 + Q1 + Q5) + Q0
= Q8 + Q6 + Q5
= Q5 + Q6 + Q8

表9は、直列クロックサイクル0～35に対応する4つの並列クロックサイクルに対する並列疑似乱数列生成機の出力値を示す。これらの出力は、最初の38の直列クロックサイクルに対する直列疑似乱数列生成機の出力段9に対応することが判る。

表9

$1 + X^3 + X^5 + X^7$ 多項式に対応する直列PRGをエミュレートする並列疑似乱数列生成機(幅=9ビット)

並列	並列	並列	並列	並列	並列	並列	並列	並列	並列	並列	並列
20,29428	20,29428	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	
0	0 - 8	0	1	1	1	1	1	1	1	1	
1	9 - 17	1	0	1	0	0	0	1	0	1	
2	18 - 26	0	1	0	0	0	1	1	1	1	
3	27 - 35	1	1	0	1	1	1	1	1	0	

以上の説明から、疑似乱数列生成機の幅が直列疑似乱数列生成機に使用されている段の数に少なくとも等しい限りは、並列疑似乱数列生成機が実現可能であることが判る。更に、並列PRGを実行するために必要な排他的ORゲートの最小数は、少なくとも並列PRGが直列PRGに等しい幅を有する場合には、対応する直列PRGに使用されている排他的ORゲートの数に必ずしも等しくないことが判る。

以下数学的解析によって、並列PRGの幅が少な

並列疑似乱数列生成機

数学的解析

1. 並列疑似乱数列生成機について

並列疑似乱数列生成機について、シフトレジスタを用いて構築されている従来の直列PRG生成機を置き換えるための解析を行なう。並列及び直列の生成機をそれぞれ第5A図及び第5B図に示した概略図によって説明する。

従来の解決策においては、P段シフトレジスタの幾つかの段から発信された信号は一緒に排他的OR(XOR)ゲートによって加えられ、得られた信号はレジスタの入力に供給され、帰還を生成する。逆流する信号値の間には方程式：

$$S_n = A_1 S_{n-1} + A_2 S_{n-2} + \dots + A_p S_{n-p} \quad (4)$$

[式中、「+」はXORまたは2を法とする加算に対して使用されており、 $A_1, \dots, A_i, \dots, A_p$ は、段*i*が接続されているならば1であり、そうでなければ0である]

くとも直列PRG多項式を実現するのに必要な段の数に等しい場合に、直列PRGの並列PRGエミュレーションが常に存在することを立証する。

が成立している。これは、係数が2を法とする整数の体(フィールド)、即ち ' $F(0,1)$ ' に含まれる方程式である。

信号を「Z変換」すると、

$$S(Z) = A_1 Z^1 S(Z) + A_2 Z^2 S(Z) + \dots + A_p Z^p S(Z) \quad (5)$$

または

$$P(Z) \cdot S(Z) = 0 \quad (6)$$

$$\text{但し: } P(Z) = Z^p + A_1 Z^1 + A_2 Z^2 + \dots + A_p Z^p \quad (7)$$

となる。方程式(5)と(6)とは等価である。

$P(Z)$ は S の特性多項式であり、 S の「生成式(generator)」と考えてもよい。

多項式 $P(Z)$ は「既約及び素」であり(係数が $F(0,1)$ に含まれる、より小さい次数の多項式の積ではない)、原始根 $Z^p + 1 = 0$ ($q = 2^p - 1$) を有し、系によって生成される数列は周期 $2^p - 1$ の疑似乱数列生成式となる。

並列生成機は、その入力信号が XOR ゲート網によって計算される多重出力ラッチ(例えば複数の

フリップフロップ)で構成されており、またラッチの出力信号はこのXORゲート網に供給される。

基本事項

以下の事項はデジタル信号処理方法を専門としない読み手に有効であろう。

1) 「2を法とする整数」の体はただ2つの元、即ち0と1とを含み、2種類の演算、即ち乗算(AND)と加算(排他的ORまたはXOR)とにおいて、

$$0 \times 0 = 0, 0 \times 1 = 1 \times 0, 1 \times 1 = 1, \text{ 及び}$$

$$0 + 0 = 0, 0 + 1 = 1 + 0 = 1, 1 + 1 = 0$$

が成立する。係数がこの体にある多項式は以下の特性を有する。即ち、

$P(Z) = Q(Z)$ は $P(Z) + Q(Z) = 0$ と等価である。また $(1+Z)^2 = 1 + Z^2$ (何故ならば $2 = 0$ である) である。

2) もし $S_n = S(nT)$ (T は時間間隔である) ならば、

$$S(Z) = \sum S_n Z^n \quad (Z \text{ は遅延演算子である})$$

であるような「Z変換」を使用する。何故ならば、

$$Z S(Z) + \sum S_n Z^{n+1} = \sum S_{n+1} Z^n$$

多くとも 2^n ワードを包含することは容易に判る。

従って多くとも $2^n - 1$ 個のヌルでないワードが存在し得、配列の周期は多くとも $2^n - 1$ である。この周期は、「既約及び素」の多項式と称される特定の多項式を用いて得られる。

5) 「 a 」を $P(Z) = 0$ の根とすると、

$$P(a) = a^0 + A_1 a^1 + A_2 a^2 + \cdots + A_n a^n =$$

$$P^2(a) = a^0 + A_1 a^1 + A_2 a^2 + \cdots + A_n a^n$$

である。これは、 $A_i = A_i$ であり、

且つ上記式の n 個の根は a, \dots, a^{n-1} であるので

a^{n-1} は $P(Z) = 0$ のもう1つの根であるが故である。

また $a^{n-1} = 1$ であるので累乗指数 2^n を有する次の根は「 a 」に等しい。

並列生成機

第5A図の並列生成機の「Z方程式」は、

$$Z^0 = A_{0,0} Z^0 + A_{0,1} Z^{n-1} + \cdots + A_{0,n-1} Z^{n-1}$$

$$Z^1 = A_{1,0} Z^0 + A_{1,1} Z^{n-1} + \cdots + A_{1,n-1} Z^{n-1}$$

であり、これは $S(t-T)$ のZ変換であるからである。

$$3) \quad S_n = A_0 S_{n-1} + A_1 S_{n-2} + \cdots + A_n S_{-1} \quad (5)$$

の解を求める場合に、通常、

$$S_n = C a^{-n} \quad [C \text{ は定数である}]$$

と置くと方程式(5)は、

$$a^{-n} = A_0 a^{-n+1} + A_1 a^{-n+2} + \cdots + A_n a^{-1}$$

$$\text{または } a^n + A_0 a + A_1 a^2 + \cdots + A_n a^n = 0$$

となり、「 a 」は $P(Z) = 0$ の根であるべきであることが判る。この方程式には n 個の根が存在する。

これらの根は一般に0または1で表わすことはできないが、式(5)の一般解はそれらの連続累乗の線形組合せとなる。即ち、

$$S_n = a_0^{-n} + a_1^{-n} + \cdots + a_n^{-n}$$

となり、これは $P(Z)$ の根の対称関数、即ちもしこれらの係数が2を法とする整数の体に含まれるならば、0または1である $P(Z)$ の係数の関数である。

4) n ビットを含む直列PNS生成機のシフトレジスタは、ヌル配列を生成するワード $0, 0, 0, \dots$ を含み

.....

$$Z^0 = A_{0,0} Z^0 + A_{0,1} Z^{n-1} + \cdots + A_{0,n-1} Z^{n-1}$$

.....

$$Z^{n-1} = A_{n-1,0} Z^0 + A_{n-1,1} Z^{n-1} + \cdots + A_{n-1,n-1} Z^{n-1}$$

である。

(その要素が $A_{i,j}$ である) 行列はラッチの2つの連続する状態 $n-1$ と n の間の遷移行列 (transition matrix) である。これらの係数は、出力 j が入力 i に一般に XOR回路によって連結されているか否かに応じて1または0となる。例えば方程式 i は、

$$S_{n-1} = (A_{1,0} S_{n-2}) \text{XOR} (A_{1,1} S_{n-2-1}) \text{XOR} (A_{1,2} S_{n-2-2}) \cdots \text{XOR} (A_{1,n-1} S_{n-2-n+1})$$

に対応しており、方程式 i は、

$$Z^i = \sum_{j=0}^{N-1} A_{i,j} Z^{n-j} \quad \text{または}$$

$$Z^0 = Z^{n-1} + A_{i,0} Z^{n-1} = Z^{n-1} R_i(Z)$$

と書くことができる。

R_i は、その係数が遷移行列の行*i*の要素である多项式である。

$T_i(Z) = Z^0 + Z^{n-1}R_i(Z)$ は、 $T_i(Z) \cdot S(Z) = 0$ であるものとなるべきである。 $P(Z) \cdot S(Z) = 0$ は既知であるので、 $T(Z)$ が $P(Z)$ の倍数であるならば、例えば $T(Z) = P(Z) \cdot Q(Z)$ であり、すると、

$$\begin{aligned} T(Z) \cdot S(Z) &= P(Z) \cdot Q(Z) \cdot S(Z) \\ &= Q(Z) [P(Z) \cdot S(Z)] = 0 \end{aligned}$$

となる。

(この結果は、 S の連続する値が $P(Z) = 0$ の根の累乗の組合せであることを考慮することにより得ることができる、これは、 $T(Z) = 0$ が少なくとも $P(Z) = 0$ と同じ根を有することを示唆する)。

ここで、多项式：

$$P = A_0 + A_1 Z + A_2 Z^2 + A_3 Z^3$$

を考える(理解し易いように特定の例を用いるが、説明方法は一般的である)。 $P(Z)$ によって生成される数列は、

数列であれば0となる。更に、もし $S'_{n-1}, S'_{n-2}, S'_{n-3}, S'_{n-4}$ が S の連続する値であるならば、計算した和は0となり、 S'_{n-1} は S の次のサンプルとなる。以上から、もし $T(Z)$ が $P(Z)$ の倍数であるならば、

- 1) 期待通り $T(X) \cdot S(Z) = 0$ であり、且つ
- 2) 「良いシード」が与えられたならば $T(Z)$ は数列 S を生成すると結論される。この結果は、数列 S の一連のサンプルを意味する(別のシードを用いても Q によって数列が生成されるであろう)。

$T(Z)$ では、(常に1である)その最初の係数とその*N*番目の最後の係数(R_i の係数)のみがゼロでないとすることができる。従って、必要とされるシードはラッチ内に含まれるサンプルに制限される。出発時には、ラッチに $P(Z)$ によって生成される数列の一部を負荷することが必要である。全ての多项式 $T_i(Z)$ はラッチの次のシリーズのビットのサンプルを生成し、各クロック時に対応して図の左側

$$A_0 S_{n-1} + A_1 S_{n-2} + A_2 S_{n-3} + A_3 S_n = 0$$

$$A_0 S_{n-1} + A_1 S_{n-2} + A_2 S_{n-3} + A_3 S_{n-4} = 0$$

$$A_0 S_{n-1} + A_1 S_{n-2} + A_2 S_{n-3} + A_3 S_{n-5} = 0$$

.....

である。 $Q(Z) = B_0 + B_1 Z + B_2 Z^2$ と置くと、

$$\begin{aligned} T(Z) &= P(Z) \cdot Q(Z) = A_0 B_0 + (A_0 B_1 + A_1 B_0) Z + \\ &\quad (A_0 B_2 + A_1 B_1 + A_2 B_0) Z^2 + (A_0 B_3 + A_1 B_2 + A_2 B_1) Z^3 \\ &\quad + (A_0 B_4 + A_1 B_3 + A_2 B_2) Z^4 + A_3 B_3 Z^5 \end{aligned}$$

$$T(Z) = C_0 + C_1 Z + C_2 Z^2 + C_3 Z^3 + C_4 Z^4 + C_5 Z^5$$

となる。

計算すると S' は数列であり、

$$\begin{aligned} C_0 S'_{n-1} + C_1 S'_{n-2} + \dots + C_5 S'_{n-6} \\ = A_0 B_0 S'_{n-1} + (A_0 B_1 + A_1 B_0) S'_{n-2} + \dots \end{aligned}$$

となる。従って、

$$\begin{aligned} B_0 (A_0 S'_{n-1} + A_1 S'_{n-2} + A_2 S'_{n-3} + A_3 S'_{n-4}) + \\ B_1 (A_0 S'_{n-2} + A_1 S'_{n-3} + A_2 S'_{n-4} + A_3 S'_{n-5}) + \\ B_2 (A_0 S'_{n-3} + A_1 S'_{n-4} + A_2 S'_{n-5} + A_3 S'_{n-6}) \end{aligned}$$

であり、この式は、 S' が $P(Z)$ によって生成される

に位置する*N*ビットシリーズ(状態*n*)は右側に位置するシリーズ(状態*n-1*)となる等が言える。

第6図は多项式 $T_i(Z)$ の係数の図である。1に等しい係数は「X」で表しており、それ以外は0に等しい。遷移行列の要素である R_i の係数は平行四辺形の内側にあり、問題となるのは、

- 1) $P(Z)$ の倍数、または $P(Z)$ によって生成される数列の生成式(これは等価である)であり、
- 2) 最初の係数を除いて平行四辺形に包含される係数を有し、
- 3) 最も単純な実行態様を与えるために最小の1に最小の項を有する

多项式を見付けることであることが判る。

「Bezoutの関係」(表10参照)は上記最初の2つの条件を満足する多项式を計算することができるが、第3の条件は常に満足するとは限らない。

「良い」多项式を見付ける極めて単純な方法は、行列の各行、即ち平行四辺形内に含まれる2つの

ゼロでない係数を有する多項式に対して「試算及び検証(try and see)」を行なうことである。これらの多項式は数列 S の生成式としてテストされ、最初に見付けられたものを使用し、可能であれば行列の次の行に対してもそれを再度使用する。2つの係数を用いた検索が失敗した場合には3つまたはそれ以上の係数に対して検索する等となる。

多項式は本来単純であるけれども、数10秒間の計算時間をすることがある(12次の多項式、 $N=32$ に対して20秒(O.E.C. VAX8600コンピュータ)を要するが、7次の多項式で $N=8$ または16に対してはほぼ即座に結果ができる)。ここで N は M 、即ち並列出力の数と等価である。

他の誘導方法

a) 並列システムの特性方程式

かかる並列生成機は、その要素が0または1(1はXOR演算を意味する)である遷移行列によって連結されているラッチの2つの連続する状態によって

で置き換える。

方程式 $S_k(Z) = 0$ は、遷移行列の全ての行 k ($1 < k < N$) に対して満足されるべき特性方程式である。

b) 特性方程式の特徴

$P(Z)$ の P 個の根の連続累乗は方程式(4)の解である。信号 S_n はこれらの累乗の線形組合せであり、 $P(Z)$ の根の対称関数である。

従って直列シフトレジスタと同じ信号を生成するためには、 $S_k(Z)$ の根は $P(Z)$ の根を包含する必要があり、

$$S_k(Z) = P(Z) Q_k(Z) \quad (12)$$

(式中、 S_k 及び P は Z 項を有するので、 $Q_k(Z)$ は少なくともかかる項を有するべき多項式である。) である。この逆は成立するであろうか。

もし式(11): $S_k(Z) = P(Z) Q_k(Z)$ であれば、 $S_k(Z) = 0$ は、 $P(Z)$ の根に対してのみでなく $Q_k(Z)$ の根に対しても真となる。ここで寄生根(parasitic root)として公知の問題が生じるが、「良いシード」(即

与えられ得る。そして、第2の状態の信号の各々は第1の状態の信号に式:

$$Z^i = \sum j B_{ij} Z^{i+j} \quad (8)$$

($0 \leq i \leq N-1$ 且つ $0 \leq j \leq N-1$ 、 $B_{ij} = 0$ または 1) によって依存する。 N はラッチ内に含まれるビット数であり、シフトレジスタによる解決策のごとき 1 直列クロックサイクル当たり 1 つのビットを与えるのではなくて、PRG の N ビット (N は前記のごとき M と等価である) のシリーズは、各並列クロックサイクルに対して発信される。 $k = N-i$ と置くと式(8)は、

$$Z^{i+j} = Z^i \sum j B_{kj} Z^j = Z^i R_k \quad (9)$$

(式中、 $R_k = \sum j B_{kj} Z^j$ は、行列の k 行(または $(N-i)$ 行)の係数を B_{kj} とする $(N-1)$ 次の多項式である) と書ける。式(8)を、

$$Z^i = I = Z^i R_k \quad (10)$$

または

$$S_k(Z) = 1 + Z^i R_k = 0 \quad (11)$$

ち良い PRG の一部分) を選択することにより、かかる寄生根の導入を回避することができる。これは、 S_n, S_{n-1} 等がラッチ内に包含され且つ PRG の一部分であるならば S_{n+1} は同じ PRG のビットであるし、もし $S_{n+1}, S_n, S_{n-1}, \dots$ が PRG の一部分であるならば S_{n+2} は PRG のビットである等、 S_n の連続する値を考慮することにより証明され得る。

全ての多項式 $S_k(Z)$ は、 Z^i から出発して $P(Z)$ の倍数であらねばならない。このような多項式は、 Z^i と Z^{i+j-1} の間にのみ他の項(P_k の項)を有し、逆に、かかる多項式は並列発生機には都合が良い。 k の同じ値に対して $S_k(Z)$ の幾つかの等価の式が存在し得る。

S_k の異なる式が存在し得、例えば以下の 2 つの多項式:

$$S_{k1}(Z) = 1 + Z^i R_{k1} = P(Z) Q_{k1}(Z) \quad (13)$$

$$S_{k2}(Z) = 1 + Z^i R_{k2} = P(Z) Q_{k2}(Z) \quad (14)$$

は有効と言える。

唯一の条件は、 P_{k1} 及び P_{k2} の次数がいずれも N より小さいことである。

上記2つの式を減算することにより、

$$S_{k1} - S_{k2} = Z^k (R_{k1} - R_{k2}) = P(Z) (Q_{k1} - Q_{k2}) \quad (15)$$

を得る。

第1に、多項式 $(S_{k1} - S_{k2})$ は $P(Z)$ で整除され、 S_{k1} 及び S_{k2} は「 $P(Z)$ を法として合同」であると見なされる。これは、 S_{k2} が $P(Z)$ を基準として S_{k1} の項を置換することにより得られることを意味する。

例えばもし $P(Z) = 1 + Z^4 + Z^8$ であれば、 S_{k1} において、 $1 + Z^4 + Z^8 = 0$ であるならば $Z + Z^4 + Z^8 = 0$ であるので、 Z を $Z^4 + Z^8$ で置き換えることができる。

第2に、ゼロ根をもたない素数である $P(Z)$ は Z^k で整除されず、 $(Q_{k1} - Q_{k2})$ は Z^k で整除される。 $(R_{k1} - R_{k2})$ もまた $P(Z)$ の倍数であり、 R_{k1} 及び R_{k2} は $P(Z)$ を法として合同である。

従って、行列の同じ行に対して等値の特性多項式 $S_k(Z)$ を与える(次数が N より小さい)「 $P(Z)$ を法

$$1 = Z^k R_k + P(Z) Q_k(Z) \quad (17)$$

BEZOUTの関係を認識する(後述の表10の「BEZOUTの関係」参照)。

$P(Z)$ 及び $Q(Z)$ を2つの多項式とすれば、それらの最大公約数(GCD)または最大公因数(HCF)は、
 $HCF(P, Q) = A(Z)P(Z) + B(Z)Q(Z) \quad (18)$

で表わされる。A及びBは(ユークリッドの互除法から説明される)極めて単純なアルゴリズムを用いて見つけることができ、Bの次数はPの次数よりも小さい。

Z^k 及び $P(Z)$ は公因数を持たないので(Pは既約である)、それらのHCFは1であり、式(17)はBEZOUTの関係である。

全ての値のkに対して、その次数が $P(Z)$ の次数 P よりも小さい多項式 R_k を決定することができる。式(17)において $k=1$ をとると $1 = ZR + PQ$ となり且つ PQ の次数は少なくとも P に等しいので、Rの次数は多くとも p に等しく、唯一の可能性はRの次数 = p 。

として合同」の幾つかの多項式 $R_k(Z)$ が存在し得る。

第6図は幾つかの問題点を示す。

1) 考慮すべき2つの座標系が存在すること:

1つは多項式 S_k に対するものであり、1つは多項式 R_k に対するものである。これらは平行四辺形の内側または辺上になくてはならず($k = 1 \sim k = 8$)、 R_k の係数1が許容される位置を「/」で記した。

2) 選択した実施例においては $P(Z)$ の2つの重要な倍数、即ち、

$$1 + X^4 + X^8 \quad \text{及び} \quad 1 + Z^4 + Z^8$$

が存在し、 S_k の非定数項は、上記倍数の全てが許容範囲内にあるならばそのうちの1つの非定数項とすることができます。

3) 幾つかの多項式 S_k は同一であり(例えば $S_1 \sim S_6$)、対応する R_k は項の平行移動のみが異なる。

C) BEZOUTの関係

$$S_k(Z) = 1 + Z^k R_k = P(Z) Q_k(Z) \quad (16)$$

または

1であり、Qの次数は0である。即ち少なくとも1つの多項式 R_k は p 個の項を有しており、遷移行列は少なくとも p 個の列を有する必要がある。

従って、

1) N は少なくとも p に等しくなければならない(N (ここで N と同じ)と p との間に見られる関係説明参照)。

2) P より大きいかまたは P に等しい N に対して、かかる問題に対する少なくとも1つの解がある。

この解は一般に、典型的には最小のXOR回路を求めるが故に最適ではない。しかし $N > p-1$ であるならば、更に次数が N より小さいという条件でBEZOUTの関係によって与えられるものを用いて $P(Z)$ を法として合同な多項式 R_k を探すことにより解を向上する方法が存在する。

d)「発見的方法(Heuristic Solution)」

発見的方法は、2つ、3つまたはそれ以上の非定

数項を有する $P(Z)$ の倍数を系統的に探索することからなる。行 k に対して 2 つの係数の解が見付かったならば、それを $k+1, \dots$ に対して出来る限り使用する。3 つ以上の係数が必要であるならば、それらを行 k に対してのみ使用し、次の行はより少ない係数を許容することが望まれるので、2 つの係数を再度用いて開始する。テストするためには $P(Z)$ で除算し、余りがゼロ多項式か調べる。これは、高い値の ρ 及び N に対しては計算時間が膨張することがあるが、いずれにせよ最速解を導くことができる(規つかの解が存在する場合がある)。少なくとも現時点では最初に見付かった解を採用する。

S_k 多項式をテストする別の方法は、多項式が所与の特性多項式によって生成された疑似乱数列を生成し得るか直接に検証することである。この方法はプログラム「GSPA-E」(表 11 及びサブルーチン POLYANCOEFX の TEST 部分参照)において使用されて

P が「良い」多項式であることを確認するため、並列システムのテストのための良い「シード」を準備するため、及び

並列システムをテストする基準を設けるために、 $P(Z)$ に対応する PRG 配列 (Seq1) を生成する。

2) 行列の要素を計算する。

3) 結果を印刷する。

行列の係数テーブル

N が 32 以下である場合には行列の図

4) 検証する。

配列 (Seq2) を生成し、Seq1 と比較する。

上記プログラムと一緒にサブルーチンファイルを使用する。サブルーチンファイルは全て本発明の目的に必要な 2 を法とする代数における全ての演算を包含する。

テーブル 12 は、GSPA-E プログラムの実行による端末リストサンプルである。

テーブル 13 は、SONET 多項式 $(1 + Z^4 + Z^7)$ の 8、

いる。

目的に応じて勿論他の方法も可能である。例えば、条件を満足し得る多項式 S_k のテーブルを計算し、そのなかから選択して行列を構築することもより優れているであろう。

勿論、 $(1 + Z^4 + Z^7)^2$ のような倍数も良いことは明らかである。

まとめ

問題は、最小の係数を有する P の倍数を認知し、そのなかから、その非定数項が P_k 多項式の範囲内にあるものを選択することである。

e) プログラム

プログラムは 4 つの部分を含む。

1) 初期化と、データ、即ち、

多項式 $P(Z)$ の次数 ρ と、

λ_0 及び λ_ρ (これらは常に 1 である) 以外の P の係数とラッチのビット数 N と

の入力を行なう。更に、

16、24、32 及び 64 ビット並列ワード幅に対する幾つかのプリントアウトを包含する。

1) 参考文献

Error Correcting Codes.

W. Wesley Peterson and E. J. Weldon (MIT Press)

Error Correction Coding for Digital Communications.

G. C. Clark and J. B. Cain (PLENUM)

Shift Register Sequences

Solomon W. Golomb (Holden-Day, Inc.)

Sequences Pseudo-Aleatoires

Georges C. Roger (Laboratories de Marcoussis, Note Interne)

State Variables for Engineers (John Wiley & Sons, Inc.)

P. Derusso, R. Roy and C. Close, pp158-186

表 10

「Bezout の関係」

2 つの整数 a 及び b 、または 2 つの多項式の最大公因数 (HCF) を求めたい場合、そのアルゴリズムはいずれに対しても同様である。

まず a を b で除算する。即ち、

$$a = q_0 b + r_1 \quad 0 \leq r_1 \leq b$$

とする。 a 及び b は HCF で割り切れ、更に r_1 も HCF で割り切れる。次に b を r_1 で除算する等を繰り返す。即ち、

$$b = q_1 r_1 + r_2 \quad 0 \leq r_2 \leq r_1$$

$$r_1 = q_2 r_2 + r_3 \quad 0 \leq r_3 \leq r_2$$

R は次第により小さくなり、従って、

$$r_{n-2} = q_{n-1} r_{n-1} + r_n$$

（ r_n は HCF である）

$$r_{n-1} = q_n r_n + r_{n+1} \quad r_{n+1} = 0$$

…

r_{n-1} は r_n で整除され、 r_{n-2} も r_n で整除され、…、

a 及び b も r_n で整除される。

従って r_n は a 及び b の HCF であり、これがユークリッドの互除法である。

次に連続する余りの数列：

$$l = a(z) \lambda(z) + b(z) \beta(z)$$

の関係が得られる。

λ_n の次数は積 $q_1 \cdot q_2 \cdots q_{n-1}$ の次数に等しく、

β_n の次数は積 $q_0 \cdot q_1 \cdots q_{n-1}$ の次数に等しいこと

は明らかであるし、計算することもできる。更に、

λ を多項式 λ の次数を意味するとすると、

$$-q_0 = -a - b$$

$$-q_2 = -b - r_1$$

$$-q_2 = -r_1 - r_2$$

…

$$-q_{n-1} = -r_{n-2} - r_{n-1}$$

$$-q_n = -r_{n-1} - r_n$$

となり、従って $-(q_0 \cdot q_1 \cdot q_2 \cdots q_{n-1}) = -a = -r_{n-1}$

である。

a 及び b が互いに素であると仮定すると、 r_n はそれらの HCF であり、 $-r_n = 0$ 及び $-r_{n-1}$ は少なくとも 1 である。従って β_n は $-a$ よりも小さく、同様の理由で λ_n は $-b$ よりも小さい。

（表 10 略わり）

$$r_1 = a - q_0 b = A_1 a + B_1 b \quad \text{但し } A_1 = 1 \text{ 及び } B_1 = -q_0$$

$$r_2 = b - q_1 r_1 = A_2 a + B_2 b \quad A_2 = -q_1 \quad A_1 \text{ 及び } B_2 = -q_1 B_1$$

$$r_3 = r_1 - q_2 r_2 = A_3 a + B_3 b$$

$$A_3 = A_1 - q_2 \quad A_2 \text{ 及び } B_3 = B_1 - q_2 \quad B_2$$

$$r_n = A_n a + B_n b$$

$$\text{但し } A_n = A_{n-2} - q_{n-1} A_{n-1} \quad A_{n-1} \text{ 及び } B_n = B_{n-2} - q_{n-1} B_{n-1}$$

故に、 A_n 及び B_n は A_1 及び B_1 から得られる。 $A_1 = 1$ 、 $B_1 = 0$ (-1 は添字である) 且つ $A_0 = 0$ 及び $B_0 = 1$ とする。 R_n 、 A_n 及び B_n を与えるアルゴリズムは、添字 1 から出発して単純に実行される。

もし R_n が HCF であるならば、「Bezout の関係」：

$$\text{HCF}(a, b) = \lambda a + \beta b$$

が得られる。

a 及び b が互いに素であるならば、 $R_n = \text{HCF}(a, b) = 1$ である。 a 及び b が多項式であるならば R_n は定数であり、係数が $F(0, 1)$ に含まれる場合には 1 に等しい定数である。そして、

三

- 147 -

CHARACTERISTIC POLYNOMIAL: : 20 26 27
K? : (RETURN=YES, IF NOT. INPUT: N) X

1) NUMBER OF SIMULTANEOUS BITS (HDP-1)? 8
K? : RETURN=YES, IF NOT, INPUT: H) Y

***** DEGREE OF CHARACTERISTIC POLYNOMIAL : 7 *****
CHARACTERISTIC POLYNOMIAL : 20 26 27
***** OF SIMULTANEOUS BITS: 4 *****

CONDUCTING

180 TERMINATION OF THE CONTRACT

\$ TY CPSA.0.A.T
 PARALLEL PSEUDONOISE SEQUENCES GENERATOR.
 COMPUTATION OF THE TRANSITION MATRIX. (PROGRAM CPSA)
 GEORGES ROGER L.O.H. 9/11/88

DEGREE OF CHARACTERISTIC POLYNOMIAL : 7
 CHARACTERISTIC POLYNOMIAL : z0 z6 z7
 NB OF SIMULTANEOUS BITS: 0

RH07	:	z3	z6
RH06	:	z4	z3
RH05	:	z3	z4
RH04	:	z2	z3
RH03	:	z1	z2
RH02	:	z0	z1
RH01	:	z3	z7
RH00	:	z4	z6

DEGREE OF CHARACTERISTIC POLYNOMIAL : 7
 CHARACTERISTIC POLYNOMIAL : z0 z6 z7
 NB OF SIMULTANEOUS BITS: 0

MATRIX:

0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7
0	-	-	-	-	-	-	-
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-

DEGREE OF CHARACTERISTIC POLYNOMIAL: 7
 CHARACTERISTIC POLYNOMIAL : z0 z6 z7
 NB OF SIMULTANEOUS BITS: 8

MATRIX:

0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7
0	-	-	-	-	-	-	-
1	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-

VERIFICATION O.K. !!!

PARALLEL PSEUDONOISE SEQUENCES GENERATOR.
 COMPUTATION OF THE TRANSITION MATRIX. (PROGRAM CPSA)
 GEORGES ROGER L.O.H. 9/11/88

DEGREE OF CHARACTERISTIC POLYNOMIAL : 7
 CHARACTERISTIC POLYNOMIAL : z0 z6 z7
 NB OF SIMULTANEOUS BITS: 8

RH07	:	z5	z6
RH06	:	z4	z5
RH05	:	z3	z4
RH04	:	z2	z3
RH03	:	z1	z2
RH02	:	z0	z1
RH01	:	z5	z7
RH00	:	z4	z6

 DEGREE OF CHARACTERISTIC POLYNOMIAL : 7
 CHARACTERISTIC POLYNOMIAL : 20 26 27
 NB OF SIMULTANEOUS BITS: 16

MATRIX:
 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
 0 - - - - - - - - - - - - - - - -
 1 - - - - - - - - - - - - - - - -
 2 - - - - - - - - - - - - - - - -
 3 - - - - - - - - - - - - - - - -
 4 - - - - - - - - - - - - - - - -
 5 - - - - - - - - - - - - - - - -
 6 - - - - - - - - - - - - - - - -
 7 - - - - - - - - - - - - - - - -
 8 - - - - - - - - - - - - - - - -
 9 - - - - - - - - - - - - - - - -
 10 - - - - - - - - - - - - - - - -
 11 - - - - - - - - - - - - - - - -
 12 - - - - - - - - - - - - - - - -
 13 - - - - - - - - - - - - - - - -
 14 - - - - - - - - - - - - - - - -
 15 - - - - - - - - - - - - - - - -

VERIFICATION O.K. !!!

PARALLEL PSEUDONOISE SEQUENCES GENERATOR.
 COMPUTATION OF THE TRANSITION MATRIX.(PROGRAM GPSA)
 GEORGES ROGER L.D.M. 9/11/88

DEGREE OF CHARACTERISTIC POLYNOMIAL : 7
 CHARACTERISTIC POLYNOMIAL : 20 26 27
 NB OF SIMULTANEOUS BITS: 16

RN15 : 25 26
 RN14 : 24 25
 RN13 : 23 24
 RN12 : 22 23
 RN11 : 21 22
 RN10 : 20 21
 RN09 : 25 27
 RN08 : 24 26
 RN07 : 21 25
 RN06 : 22 24
 RN05 : 21 23
 RN04 : 20 22
 RN03 : 21 25
 RN02 : 21 26
 RN01 : 20 22
 RN00 : 20 22

PARALLEL PSEUDONOISE SEQUENCES GENERATOR.
 COMPUTATION OF THE TRANSITION MATRIX.(PROGRAM GPSA)
 GEORGES ROGER L.D.M. 9/11/88

DEGREE OF CHARACTERISTIC POLYNOMIAL : 7
 CHARACTERISTIC POLYNOMIAL : 20 26 27
 NB OF SIMULTANEOUS BITS: 24

RN23 : 25 26
 RN22 : 24 25
 RN21 : 23 24
 RN20 : 22 23
 RN19 : 21 22
 RN18 : 20 21
 RN17 : 25 27
 RN16 : 24 26
 RN15 : 23 25
 RN14 : 22 24
 RN13 : 21 23
 RN12 : 20 22
 RN11 : 21 215
 RN10 : 210 214
 RN09 : 29 213
 RN08 : 28 212
 RN07 : 27 211
 RN06 : 26 210
 RN05 : 25 29
 RN04 : 24 18
 RN03 : 23 27
 RN02 : 22 26
 RN01 : 21 25
 RN00 : 20 22

 DEGREE OF CHARACTERISTIC POLYNOMIAL : 7
 CHARACTERISTIC POLYNOMIAL : z0 z6 z7
 NB OF SIMULTANEOUS BITS: 24

MATRIX:

0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	2	2	3
0	1	2	3	4	5	6	7	8	9	0	1	1	1	1	1	1	1	1	1	1	1	1	2	3	
1	+	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
2	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
3	-	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
4	-	-	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
5	-	-	-	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
6	-	-	-	-	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	
7	-	-	-	-	-	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-	
8	-	-	-	-	-	-	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	
9	-	-	-	-	-	-	-	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	
10	-	-	-	-	-	-	-	-	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	
11	-	-	-	-	-	-	-	-	-	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	
12	+	-	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
13	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
14	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
15	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
16	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
17	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
18	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
19	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
20	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	
21	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	
22	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-	
23	+	+	+	+	+	+	+	+	+	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	

VERIFICATION O.K. !!!

PARALLEL PSEUDONOISE SEQUENCES GENERATOR,
 COMPUTATION OF THE TRANSITION MATRIX.(PROGRAM GFSI)
 GEORGES ROGER L.D.M. 9/11/88

DEGREE OF CHARACTERISTIC POLYNOMIAL : 7

CHARACTERISTIC POLYNOMIAL : z0 z6 z7

NB OF SIMULTANEOUS BITS: 32

RN31 : z5 z6
 RN30 : z4 z5
 RN29 : z3 z4
 RN28 : z2 z3
 RN27 : z1 z2
 RN26 : z0 z1
 RN25 : z5 z7
 RN24 : z4 z6
 RN23 : z3 z5
 RN22 : z2 z4
 RN21 : z1 z3
 RN20 : z0 z2
 RN19 : z11 z15
 RN18 : z10 z14
 RN17 : z9 z13
 RN16 : z8 z12
 RN15 : z7 z11
 RN14 : z6 z10
 RN13 : z5 z9
 RN12 : z4 z8
 RN11 : z3 z7
 RN10 : z2 z6
 RN9 : z1 z5
 RN08 : z0 z4
 RN07 : z1 z8
 RN06 : z0 z17
 RN05 : z0 z26
 RN04 : z7 z25
 RN03 : z6 z24
 RN02 : z5 z23
 RN01 : z4 z22
 RN00 : z3 z21

PARALLEL PSEUDORANDOM SEQUENCES GENERATOR.

COMPUTATION OF THE TRANSITION MATRIX. (PROGRAM OPERA)

GEORGES ROGER L.D.R. 9/11/88

DEGREE OF CHARACTERISTIC POLYNOMIAL : 7

CHARACTERISTIC POLYNOMIAL : 20 26 27

NB OF SIMULTANEOUS BITS : 64

RN63 : 26

RN62 : 24 35

RN61 : 23 24

RN60 : 22 23

RN59 : 21 22

RN58 : 20 21

RN57 : 19 20

RN56 : 18 26

RN55 : 13 25

RN54 : 12 24

RN53 : 11 23

RN52 : 10 22

RN51 : 11 216

RN50 : 210 214

RN49 : 29 213

RN48 : 18 212

RN47 : 17 211

RN46 : 16 210

RN45 : 15 205

RN44 : 14 204

RN43 : 13 203

RN42 : 12 202

RN41 : 11 201

RN40 : 10 200

RN39 : 9 198

RN38 : 8 197

RN37 : 7 196

RN36 : 6 195

RN35 : 5 194

RN34 : 4 193

RN33 : 3 192

RN32 : 2 191

RN31 : 1 190

RN30 : 11 119

RN29 : 10 118

RN28 : 9 117

RN27 : 8 116

RN26 : 7 115

RN25 : 6 114

RN24 : 5 113

RN23 : 4 112

RN22 : 3 111

RN21 : 2 110

RN20 : 1 109

RN19 : 11 108

RN18 : 10 107

RN17 : 9 106

RN16 : 8 105

RN15 : 7 104

MATRIX:

W₁ P₁ W₂ P₂ W₃ P₃ W₄ P₄ W₅ P₅ W₆ P₆ W₇ P₇ W₈ P₈ W₉ P₉ W₁₀ P₁₀ W₁₁ P₁₁ W₁₂ P₁₂ W₁₃ P₁₃ W₁₄ P₁₄ W₁₅ P₁₅ W₁₆ P₁₆ W₁₇ P₁₇ W₁₈ P₁₈ W₁₉ P₁₉ W₂₀ P₂₀ W₂₁ P₂₁ W₂₂ P₂₂ W₂₃ P₂₃ W₂₄ P₂₄ W₂₅ P₂₅ W₂₆ P₂₆ W₂₇ P₂₇ W₂₈ P₂₈ W₂₉ P₂₉ W₃₀ P₃₀ W₃₁ P₃₁ W₃₂ P₃₂ W₃₃ P₃₃ W₃₄ P₃₄ W₃₅ P₃₅ W₃₆ P₃₆ W₃₇ P₃₇ W₃₈ P₃₈ W₃₉ P₃₉ W₄₀ P₄₀ W₄₁ P₄₁ W₄₂ P₄₂ W₄₃ P₄₃ W₄₄ P₄₄ W₄₅ P₄₅ W₄₆ P₄₆ W₄₇ P₄₇ W₄₈ P₄₈ W₄₉ P₄₉ W₅₀ P₅₀ W₅₁ P₅₁ W₅₂ P₅₂ W₅₃ P₅₃ W₅₄ P₅₄ W₅₅ P₅₅ W₅₆ P₅₆ W₅₇ P₅₇ W₅₈ P₅₈ W₅₉ P₅₉ W₆₀ P₆₀ W₆₁ P₆₁ W₆₂ P₆₂ W₆₃ P₆₃ W₆₄ P₆₄ W₆₅ P₆₅ W₆₆ P₆₆ W₆₇ P₆₇ W₆₈ P₆₈ W₆₉ P₆₉ W₇₀ P₇₀ W₇₁ P₇₁ W₇₂ P₇₂ W₇₃ P₇₃ W₇₄ P₇₄ W₇₅ P₇₅ W₇₆ P₇₆ W₇₇ P₇₇ W₇₈ P₇₈ W₇₉ P₇₉ W₈₀ P₈₀ W₈₁ P₈₁ W₈₂ P₈₂ W₈₃ P₈₃ W₈₄ P₈₄ W₈₅ P₈₅ W₈₆ P₈₆ W₈₇ P₈₇ W₈₈ P₈₈ W₈₉ P₈₉ W₉₀ P₉₀ W₉₁ P₉₁ W₉₂ P₉₂ W₉₃ P₉₃ W₉₄ P₉₄ W₉₅ P₉₅ W₉₆ P₉₆ W₉₇ P₉₇ W₉₈ P₉₈ W₉₉ P₉₉ W₁₀₀ P₁₀₀ W₁₀₁ P₁₀₁ W₁₀₂ P₁₀₂ W₁₀₃ P₁₀₃ W₁₀₄ P₁₀₄ W₁₀₅ P₁₀₅ W₁₀₆ P₁₀₆ W₁₀₇ P₁₀₇ W₁₀₈ P₁₀₈ W₁₀₉ P₁₀₉ W₁₁₀ P₁₁₀ W₁₁₁ P₁₁₁ W₁₁₂ P₁₁₂ W₁₁₃ P₁₁₃ W₁₁₄ P₁₁₄ W₁₁₅ P₁₁₅ W₁₁₆ P₁₁₆ W₁₁₇ P₁₁₇ W₁₁₈ P₁₁₈ W₁₁₉ P₁₁₉ W₁₂₀ P₁₂₀ W₁₂₁ P₁₂₁ W₁₂₂ P₁₂₂ W₁₂₃ P₁₂₃ W₁₂₄ P₁₂₄ W₁₂₅ P₁₂₅ W₁₂₆ P₁₂₆ W₁₂₇ P₁₂₇ W₁₂₈ P₁₂₈ W₁₂₉ P₁₂₉ W₁₃₀ P₁₃₀ W₁₃₁ P₁₃₁ W₁₃₂ P₁₃₂ W₁₃₃ P₁₃₃ W₁₃₄ P₁₃₄ W₁₃₅ P₁₃₅ W₁₃₆ P₁₃₆ W₁₃₇ P₁₃₇ W₁₃₈ P₁₃₈ W₁₃₉ P₁₃₉ W₁₄₀ P₁₄₀ W₁₄₁ P₁₄₁ W₁₄₂ P₁₄₂ W₁₄₃ P₁₄₃ W₁₄₄ P₁₄₄ W₁₄₅ P₁₄₅ W₁₄₆ P₁₄₆ W₁₄₇ P₁₄₇ W₁₄₈ P₁₄₈ W₁₄₉ P₁₄₉ W₁₅₀ P₁₅₀ W₁₅₁ P₁₅₁ W₁₅₂ P₁₅₂ W₁₅₃ P₁₅₃ W₁₅₄ P₁₅₄ W₁₅₅ P₁₅₅ W₁₅₆ P₁₅₆ W₁₅₇ P₁₅₇ W₁₅₈ P₁₅₈ W₁₅₉ P₁₅₉ W₁₆₀ P₁₆₀ W₁₆₁ P₁₆₁ W₁₆₂ P₁₆₂ W₁₆₃ P₁₆₃ W₁₆₄ P₁₆₄ W₁₆₅ P₁₆₅ W₁₆₆ P₁₆₆ W₁₆₇ P₁₆₇ W₁₆₈ P₁₆₈ W₁₆₉ P₁₆₉ W₁₇₀ P₁₇₀ W₁₇₁ P₁₇₁ W₁₇₂ P₁₇₂ W₁₇₃ P₁₇₃ W₁₇₄ P₁₇₄ W₁₇₅ P₁₇₅ W₁₇₆ P₁₇₆ W₁₇₇ P₁₇₇ W₁₇₈ P₁₇₈ W₁₇₉ P₁₇₉ W₁₈₀ P₁₈₀ W₁₈₁ P₁₈₁ W₁₈₂ P₁₈₂ W₁₈₃ P₁₈₃ W₁₈₄ P₁₈₄ W₁₈₅ P₁₈₅ W₁₈₆ P₁₈₆ W₁₈₇ P₁₈₇ W₁₈₈ P₁₈₈ W₁₈₉ P₁₈₉ W₁₉₀ P₁₉₀ W₁₉₁ P₁₉₁ W₁₉₂ P₁₉₂ W₁₉₃ P₁₉₃ W₁₉₄ P₁₉₄ W₁₉₅ P₁₉₅ W₁₉₆ P₁₉₆ W₁₉₇ P₁₉₇ W₁₉₈ P₁₉₈ W₁₉₉ P₁₉₉ W₂₀₀ P₂₀₀ W₂₀₁ P₂₀₁ W₂₀₂ P₂₀₂ W₂₀₃ P₂₀₃ W₂₀₄ P₂₀₄ W₂₀₅ P₂₀₅ W₂₀₆ P₂₀₆ W₂₀₇ P₂₀₇ W₂₀₈ P₂₀₈ W₂₀₉ P₂₀₉ W₂₁₀ P₂₁₀ W₂₁₁ P₂₁₁ W₂₁₂ P₂₁₂ W₂₁₃ P₂₁₃ W₂₁₄ P₂₁₄ W₂₁₅ P₂₁₅ W₂₁₆ P₂₁₆ W₂₁₇ P₂₁₇ W₂₁₈ P₂₁₈ W₂₁₉ P₂₁₉ W₂₂₀ P₂₂₀ W₂₂₁ P₂₂₁ W₂₂₂ P₂₂₂ W₂₂₃ P₂₂₃ W₂₂₄ P₂₂₄ W₂₂₅ P₂₂₅ W₂₂₆ P₂₂₆ W₂₂₇ P₂₂₇ W₂₂₈ P₂₂₈ W₂₂₉ P₂₂₉ W₂₃₀ P₂₃₀ W₂₃₁ P₂₃₁ W₂₃₂ P₂₃₂ W₂₃₃ P₂₃₃ W₂₃₄ P₂₃₄ W₂₃₅ P₂₃₅ W₂₃₆ P₂₃₆ W₂₃₇ P₂₃₇ W₂₃₈ P₂₃₈ W₂₃₉ P₂₃₉ W₂₄₀ P₂₄₀ W₂₄₁ P₂₄₁ W₂₄₂ P₂₄₂ W₂₄₃ P₂₄₃ W₂₄₄ P₂₄₄ W₂₄₅ P₂₄₅ W₂₄₆ P₂₄₆ W₂₄₇ P₂₄₇ W₂₄₈ P₂₄₈ W₂₄₉ P₂₄₉ W₂₅₀ P₂₅₀ W₂₅₁ P₂₅₁ W₂₅₂ P₂₅₂ W₂₅₃ P₂₅₃ W₂₅₄ P₂₅₄ W₂₅₅ P₂₅₅ W₂₅₆ P₂₅₆ W₂₅₇ P₂₅₇ W₂₅₈ P₂₅₈ W₂₅₉ P₂₅₉ W₂₆₀ P₂₆₀ W₂₆₁ P₂₆₁ W₂₆₂ P₂₆₂ W₂₆₃ P₂₆₃ W₂₆₄ P₂₆₄ W₂₆₅ P₂₆₅ W₂₆₆ P₂₆₆ W₂₆₇ P₂₆₇ W₂₆₈ P₂₆₈ W₂₆₉ P₂₆₉ W₂₇₀ P₂₇₀ W₂₇₁ P₂₇₁ W₂₇₂ P₂₇₂ W₂₇₃ P₂₇₃ W₂₇₄ P₂₇₄ W₂₇₅ P₂₇₅ W₂₇₆ P₂₇₆ W₂₇₇ P₂₇₇ W₂₇₈ P₂₇₈ W₂₇₉ P₂₇₉ W₂₈₀ P₂₈₀ W₂₈₁ P₂₈₁ W₂₈₂ P₂₈₂ W₂₈₃ P₂₈₃ W₂₈₄ P₂₈₄ W₂₈₅ P₂₈₅ W₂₈₆ P₂₈₆ W₂₈₇ P₂₈₇ W₂₈₈ P₂₈₈ W₂₈₉ P₂₈₉ W₂₉₀ P₂₉₀ W₂₉₁ P₂₉₁ W₂₉₂ P₂₉₂ W₂₉₃ P₂₉₃ W₂₉₄ P₂₉₄ W₂₉₅ P₂₉₅ W₂₉₆ P₂₉₆ W₂₉₇ P₂₉₇ W₂₉₈ P₂₉₈ W₂₉₉ P₂₉₉ W₃₀₀ P₃₀₀ W₃₀₁ P₃₀₁ W₃₀₂ P₃₀₂ W₃₀₃ P₃₀₃ W₃₀₄ P₃₀₄ W₃₀₅ P₃₀₅ W₃₀₆ P₃₀₆ W₃₀₇ P₃₀₇ W₃₀₈ P₃₀₈ W₃₀₉ P₃₀₉ W₃₁₀ P₃₁₀ W₃₁₁ P₃₁₁ W₃₁₂ P₃₁₂ W₃₁₃ P₃₁₃ W₃₁₄ P₃₁₄ W₃₁₅ P₃₁₅ W₃₁₆ P₃₁₆ W₃₁₇ P₃₁₇ W₃₁₈ P₃₁₈ W₃₁₉ P₃₁₉ W₃₂₀ P₃₂₀ W₃₂₁ P₃₂₁ W₃₂₂ P₃₂₂ W₃₂₃ P₃₂₃ W₃₂₄ P₃₂₄ W₃₂₅ P₃₂₅ W₃₂₆ P₃₂₆ W₃₂₇ P₃₂₇ W₃₂₈ P₃₂₈ W₃₂₉ P₃₂₉ W₃₃₀ P₃₃₀ W₃₃₁ P₃₃₁ W₃₃₂ P₃₃₂ W₃₃₃ P₃₃₃ W₃₃₄ P₃₃₄ W₃₃₅ P₃₃₅ W₃₃₆ P₃₃₆ W₃₃₇ P₃₃₇ W₃₃₈ P₃₃₈ W₃₃₉ P₃₃₉ W₃₄₀ P₃₄₀ W₃₄₁ P₃₄₁ W₃₄₂ P₃₄₂ W₃₄₃ P₃₄₃ W₃₄₄ P₃₄₄ W₃₄₅ P₃₄₅ W₃₄₆ P₃₄₆ W₃₄₇ P₃₄₇ W₃₄₈ P₃₄₈ W₃₄₉ P₃₄₉ W₃₅₀ P₃₅₀ W₃₅₁ P₃₅₁ W₃₅₂ P₃₅₂ W₃₅₃ P₃₅₃ W₃₅₄ P₃₅₄ W₃₅₅ P₃₅₅ W₃₅₆ P₃₅₆ W₃₅₇ P₃₅₇ W₃₅₈ P₃₅₈ W₃₅₉ P₃₅₉ W₃₆₀ P₃₆₀ W₃₆₁ P₃₆₁ W₃₆₂ P₃₆₂ W₃₆₃ P₃₆₃ W₃₆₄ P₃₆₄ W₃₆₅ P₃₆₅ W₃₆₆ P₃₆₆ W₃₆₇ P₃₆₇ W₃₆₈ P₃₆₈ W₃₆₉ P₃₆₉ W₃₇₀ P₃₇₀ W₃₇₁ P₃₇₁ W₃₇₂ P₃₇₂ W₃₇₃ P₃₇₃ W₃₇₄ P₃₇₄ W₃₇₅ P₃₇₅ W₃₇₆ P₃₇₆ W₃₇₇ P₃₇₇ W₃₇₈ P₃₇₈ W₃₇₉ P₃₇₉ W₃₈₀ P₃₈₀ W₃₈₁ P₃₈₁ W₃₈₂ P₃₈₂ W₃₈₃ P₃₈₃ W₃₈₄ P₃₈₄ W₃₈₅ P₃₈₅ W₃₈₆ P₃₈₆ W₃₈₇ P₃₈₇ W₃₈₈ P₃₈₈ W₃₈₉ P₃₈₉ W₃₉₀ P₃₉₀ W₃₉₁ P₃₉₁ W₃₉₂ P₃₉₂ W₃₉₃ P₃₉₃ W₃₉₄ P₃₉₄ W₃₉₅ P₃₉₅ W₃₉₆ P₃₉₆ W₃₉₇ P₃₉₇ W₃₉₈ P₃₉₈ W₃₉₉ P₃₉₉ W₄₀₀ P₄₀₀ W₄₀₁ P₄₀₁ W₄₀₂ P₄₀₂ W₄₀₃ P₄₀₃ W₄₀₄ P₄₀₄ W₄₀₅ P₄₀₅ W₄₀₆ P₄₀₆ W₄₀₇ P₄₀₇ W₄₀₈ P₄₀₈ W₄₀₉ P₄₀₉ W₄₁₀ P₄₁₀ W₄₁₁ P₄₁₁ W₄₁₂ P₄₁₂ W₄₁₃ P₄₁₃ W₄₁₄ P₄₁₄ W₄₁₅ P₄₁₅ W₄₁₆ P₄₁₆ W₄₁₇ P₄₁₇ W₄₁₈ P₄₁₈ W₄₁₉ P₄₁₉ W₄₂₀ P₄₂₀ W₄₂₁ P₄₂₁ W₄₂₂ P₄₂₂ W₄₂₃ P₄₂₃ W₄₂₄ P₄₂₄ W₄₂₅ P₄₂₅ W₄₂₆ P₄₂₆ W₄₂₇ P₄₂₇ W₄₂₈ P₄₂₈ W₄₂₉ P₄₂₉ W₄₃₀ P₄₃₀ W₄₃₁ P₄₃₁ W₄₃₂ P₄₃₂ W₄₃₃ P₄₃₃ W₄₃₄ P₄₃₄ W₄₃₅ P₄₃₅ W₄₃₆ P₄₃₆ W₄₃₇ P₄₃₇ W₄₃₈ P₄₃₈ W₄₃₉ P₄₃₉ W₄₄₀ P₄₄₀ W₄₄₁ P₄₄₁ W₄₄₂ P₄₄₂ W₄₄₃ P₄₄₃ W₄₄₄ P₄₄₄ W₄₄₅ P₄₄₅ W₄₄₆ P₄₄₆ W₄₄₇ P₄₄₇ W₄₄₈ P₄₄₈ W₄₄₉ P₄₄₉ W₄₅₀ P₄₅₀ W₄₅₁ P₄₅₁ W₄₅₂ P₄₅₂ W₄₅₃ P₄₅₃ W₄₅₄ P₄₅₄ W₄₅₅ P₄₅₅ W₄₅₆ P₄₅₆ W₄₅₇ P₄₅₇ W₄₅₈ P₄₅₈ W₄₅₉ P₄₅₉ W₄₆₀ P₄₆₀ W₄₆₁ P₄₆₁ W₄₆₂ P₄₆₂ W₄₆₃ P₄₆₃ W₄₆₄ P₄₆₄ W₄₆₅ P₄₆₅ W₄₆₆ P	

前記本発明の目的及び先の説明から明らかとなつた目的は効果的に得られることは明らかであり、本発明の並列疑似乱数列発生機の範囲から離れずとも上記構成及び構造において所定の変更がなされ得るので、前記説明に含まれるまたは添付の図面に示された全ての事項は説明のためのものであつて制限的ではないと解釈されたい。

更に、特許請求の範囲は、本明細書に記載の並列疑似乱数列発生機の一般的な及び特定の性質の全てを包含するものとし、本発明の範囲の全ての説明は、文字通りこのなかに含まれるものとする。

4. 図面の簡単な説明

第1図は次に生成される値が多項式 $1 + x^n + x^m$ によって定義されるように P段シフトレジスタとして接続されている D型フリップフロップの使用を組み込んである直列疑似乱数列発生器を示す図。

20…直列疑似乱致列発生板、24…並列疑似乱致列発生板、26…ラッチ、28,30,30'…排他的ORゲート。

第2図は第5B図に示された直列PRGをエミュレートする8ビット並列PRGを示すブロック図、第3図はクロック信号を含む第2図に示された8ビット並列PRGの概略図、第4図は第1図に示された直列PRGの16ビット並列PRGの実現態様のブロック図、第5A図は、段 α と段 $\alpha-1$ との間の帰還関係を示す第5B図に示された直列疑似乱数列発生機の W 個の出力を有する並列PRGの実現態様の概略図、第5B図は段 P 及び段 $P-1$ が段1の次の値を決定するために使用される帰還値である第1図に示されたものと同様の直列PRGの概略図、第6図は第5A図に示された並列PRGに対応する直列疑似乱数列発生機の並列実施態様の一般解のための遷移行列、第7図は多項式 $1 + X^4 + X^7$ のための出力 (n) と出力 $(n+5)$ 及び出力 $(n+7)$ の値との関係を示す図、並びに第8図は多項式 $1 + X^2 + X^3 + X^6$ のための出力 (n) と出力 $(n+2)$ 、出力 $(n+5)$ 及び出力 $(n+9)$ の値との関係を示す図である。

図面の添字(内容に変更なし)

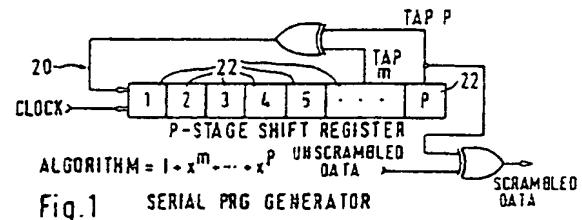


Fig.1 SERIAL PRG GENERATOR

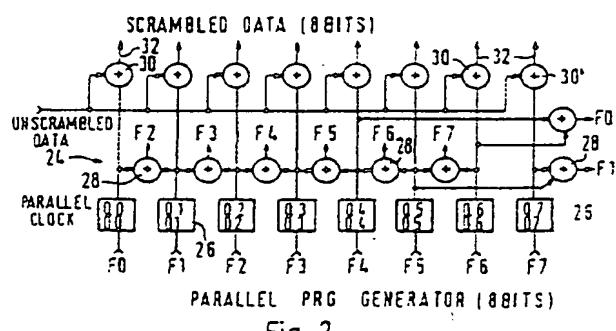


Fig. 2

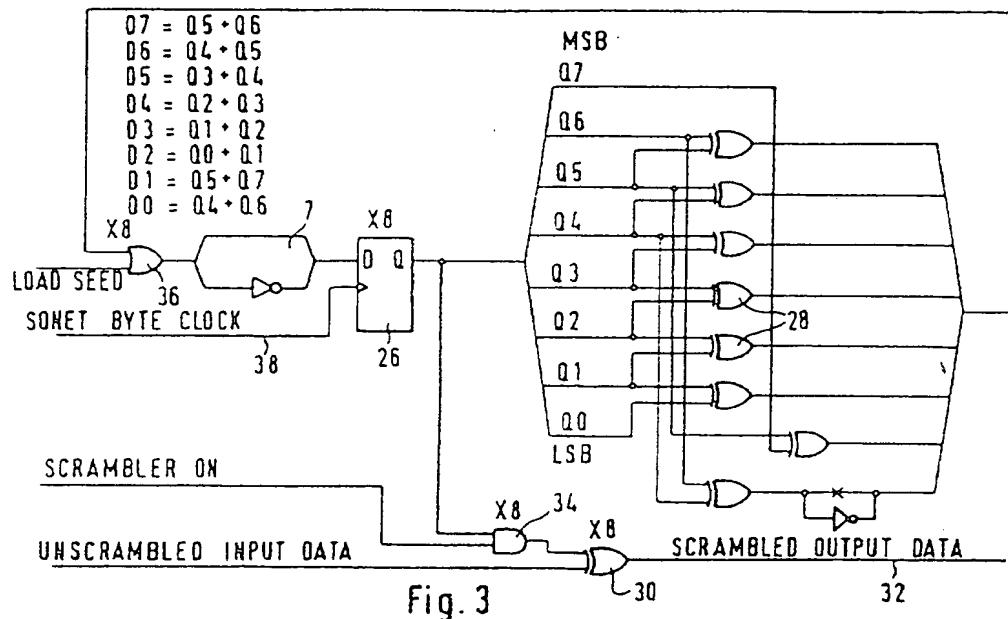


Fig. 3

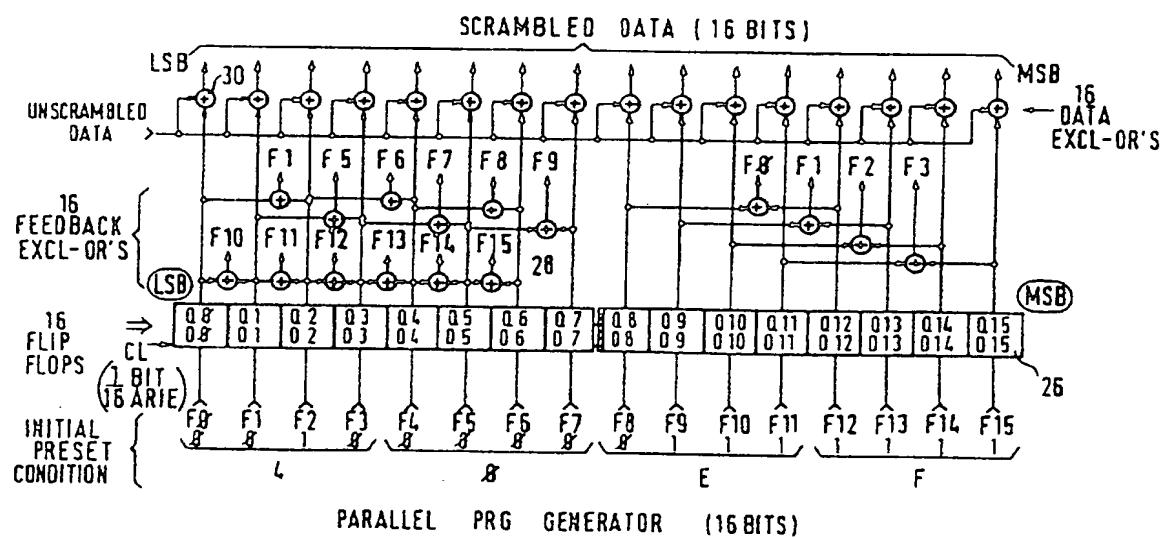
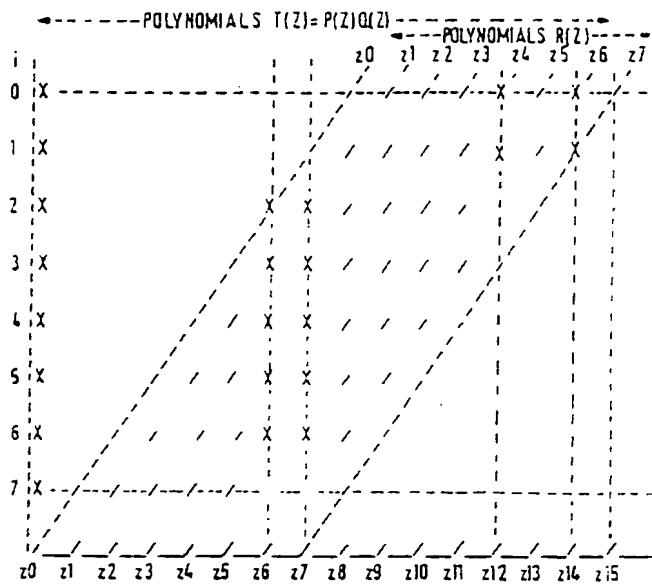


Fig. 4

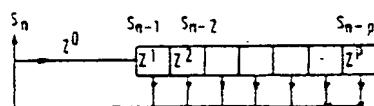
Fig. 6



RELATIVE POSITION OF THE MATRIX ELEMENTS ('X')
 AND OF POLYNOMIALS $T(z) = P(z)Q(z)$.
 THE MATRIX IS IN THE PARALLELOGRAM

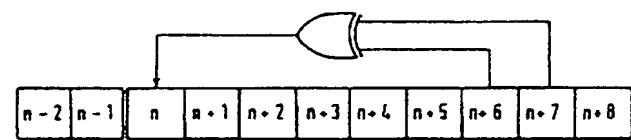
1) SHIFT REGISTER

Fig. 5B



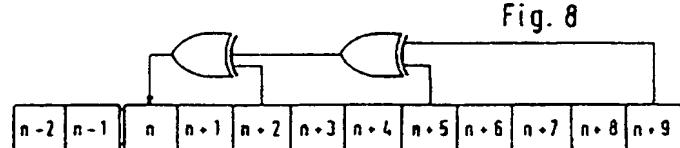
2) PARALLEL GENERATOR

Fig. 5A



$$Q(n) = Q(n+6) + Q(n+7)$$

Fig. 7



$$Q(n) = Q(n+2) + Q(n+5) + Q(n+9)$$

Fig. 8

第1頁の続き

②発明者 ジヨルジュ・アンド
レ・シヤルル・ロジエ フランス国、91240・サン・ミシエル・スユル・オルジ
ユ、バルク・ドウ・ロルモイ、バビオン・マルグリット
(番地なし)

手続補正書(方式)

平成2年9月4日

特許庁長官 横松 敏 肇

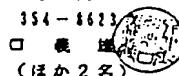


1. 事件の表示 平成2年特許願第122861号/

2. 発明の名称 直列疑似乱数列生成機をエミュレートするための並列疑似乱数列生成機及びその実行方法

3. 補正をする者
事件との関係 特許出願人

名 称 アルカテル・エヌ・ベー

4. 代 理 人 東京都新宿区新宿1丁目1番14号 山田ビル
(郵便番号 160) 電話 (03) 354-8623
(5200) 弁理士 川口義雄
(ほか2名)

5. 補正指令の日付 平成2年8月28日

6. 補正の対象 図面

7. 補正の内容

(1) 黒色で鮮明に描いた適正な図面を別紙の通り補充する。
(内容に変更なし)